

CSE508

Network Security



2023-04-18

Social Engineering

Michalis Polychronakis

Stony Brook University



Social Engineering

Exploit human behavior to breach security

Psychological manipulation of people into performing actions or divulging confidential information

"...the art and science of getting people to comply with your wishes"

"A euphemism for non-technical or low-technology means (lies, impersonation, tricks, bribes, blackmail, and threats) used to attack information systems"

Human-based deception

Take advantage of the victim's ignorance and the natural human inclination to be helpful and liked

Technology-based deception

Trick users into believing that they are interacting with a "real" computer system and are experiencing "legitimate" behavior

Basic Types of Social Engineering

Phishing

Sending emails appearing to be from reputable sources with the goal of influencing or gaining personal information

Example: emails, text messages, websites, ...

Voice/phone phishing

Eliciting information or influencing action by talking to someone over the phone

Example: call to reset password, transfer phone number, change credit card, ...

Impersonation

Pretending to be another person, or pretexting, with the goal of gaining physical access to a system or building

Example: pose as delivery persons, fire marshals, technicians, ...

Address Obfuscation

Misspelled/similar domain names (typosquatting)

From: info@paypa1.com

<http://www.citybank.com>

Misleading <A> tags

<https://www.attacker.com>><https://www.bank.com>

Seemingly legitimate/long/complex URLs

<https://www.bankofamerica.com.attacker.net/signinoptions/...>

<https://myaccount.google.com-securitysettingpage.tk/security/...>



Google

Sign in

with your Google Account

Email or phone

[Forgot email?](#)

Not your computer? Use Guest mode to sign in privately. [Learn more](#)

[Create account](#) [NEXT](#)

Address Obfuscation

Homographs, internationalized domain names (IDN), punycode

<http://ebay.com> (<http://xn--eby-7cd.com/>) – Cyrillic “a” vs. Latin “a”

Most browsers now display IDNs only for the system’s configured language

Punycode is shown if a non-default language or mixed languages are used

Dot-less addresses and other URL encoding tricks

www.cs.stonybrook.edu → <http://130.245.27.2> → <http://2197101314>

URL shorteners and redirection chains

<https://bit.ly/1PibSU0> → <https://definitely-not-a-phishing-site.com>

Completely hide the actual destination URL (even hovering doesn’t work)

Phishing or Real?

<https://github.com/kubernetes/archive/refs/tags/@v1271.zip>

<https://github.com/kubernetes/archive/refs/tags/v1.27.1.zip>

Phishing or Real?

<https://github.com/kubernetes/archive/refs/tags/@v1271.zip>

<https://github.com/kubernetes/archive/refs/tags/v1.27.1.zip>

/ U+002F

/ U+2044

/ U+2215

} *Not treated as forward slashes,
but allowed in hostnames*

The Real Culprit: @

<https://github.com/kubernetes/archive/refs/tags/@v1271.zip>

<https://drive.google.com@1157586937>

http://www.visa.com:UserSession=2f6q988316484495&usersoption=SecurityUpdate&From@61.252.126.191/verified_by_visa.html

RFC 1738: Common Internet Scheme Syntax

<scheme>://<user>:<password>@<host>:<port>/<url-path>

Section 3.3 defines the HTTP scheme as follows:

http://<host>:<port>/<path>?<searchpart>

The RFC specifically states that “No user name or password is allowed”

Browsers simply discard anything before the “@” sign

Relic of old times for FTP, TELNET, and other obsolete protocols

Domains like .zip are not really the problem

“@” is widely abused in phishing campaigns

Not really used in practice (maybe browsers should stop supporting it)

Typosquatting and Fake URLs

Besides phishing: opportunistic “hijacking” of typos when writing a website address into the URL bar

Misspelling or foreign language spelling: [exemple.com](#)

Common typos/permutations: [examlpe.com](#)

Differently phrased names: [examples.com](#)

Different top-level domains: [example.org](#), [example.cm](#), [example.co](#), ...

Many other variations

Combosquatting: combining seemingly legitimate/gripe/random words: [example-security.com](#), [example-sucks.com](#), [examplenext.com](#), ...

Doppelganger domains by omitting a period: [financeexample.com](#) (instead of [finance.example.com](#))

Extra period: [e.xample.com](#)

Typosquatting: Beyond Domain Names

NPM packages, Rust crates, ...

Typos

Name variations

Misleading names

Example:

malicious Roblox API wrapper NPM packages

Legitimate name: **noblox.js-proxied**

Malicious names: **noblox.js-proxies**

noblox.js-proxy

The screenshot shows the NPM package page for `noblox.js-proxies`. The package is version 1.0.3, published 5 days ago, and is public. It has 8 dependencies and 0 dependents. The package description is "A Node.js wrapper for interacting with the Roblox API; forked from `roblox.js`". The package is licensed under MIT. The page also shows the repository URL, homepage, and weekly downloads (59). The package is 657 kB in size and has 224 total files. There are 0 issues and 0 pull requests. The last publish was 5 days ago.

Version	License
1.0.3	MIT

Unpacked Size	Total Files
657 kB	224

Issues	Pull Requests
0	0

Spear Phishing

Meticulously prepared, carefully personalized, highly convincing messages targeted to specific individuals

- Seemingly coming from trusted colleagues/sources

- May come from their real accounts if they have been compromised

- Personalized according to their target: mention real names, personal and business information, recent activity (e.g., real purchases), ...

Highly effective! Used extensively in targeted attacks

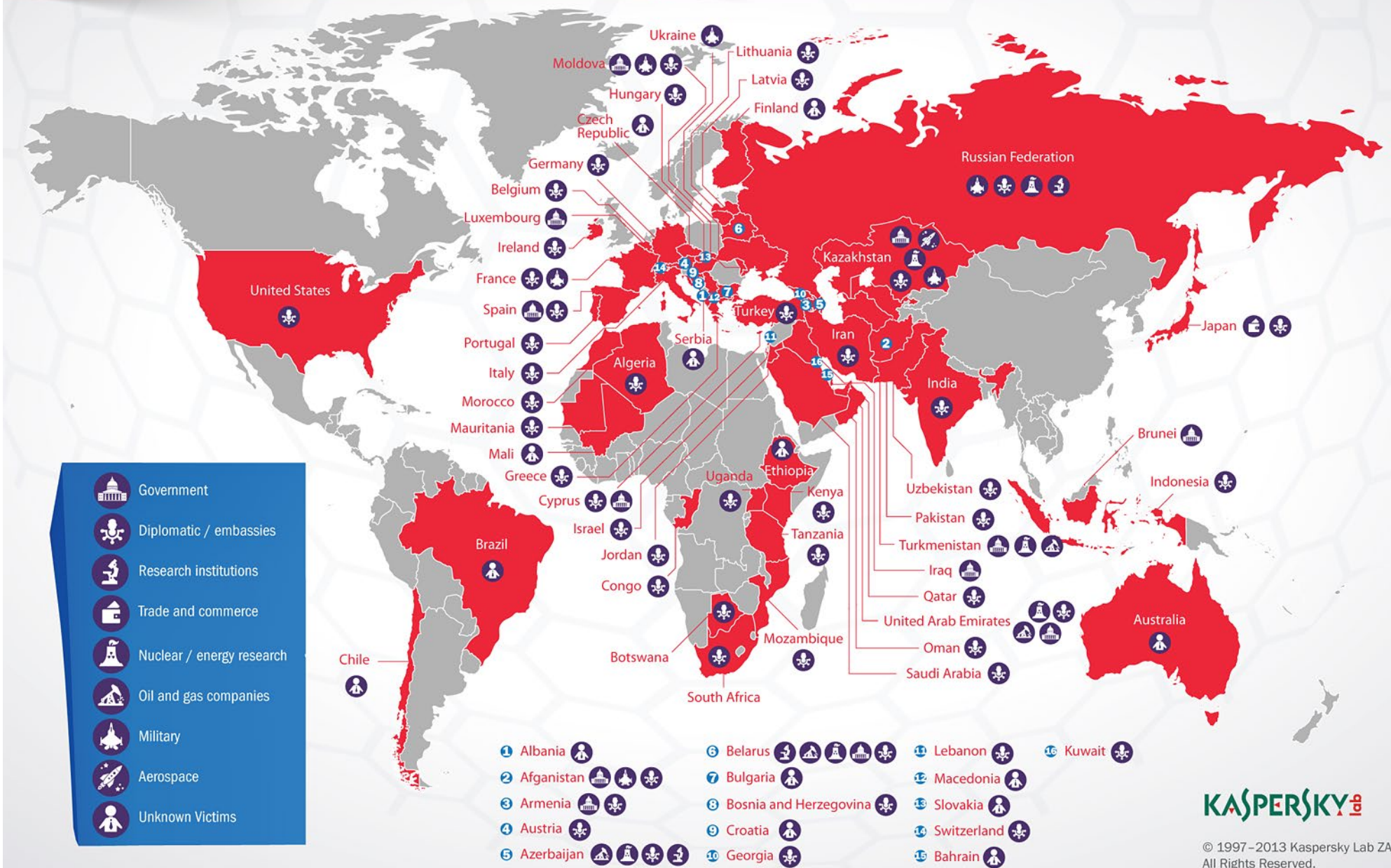
- Document attachments exploiting 0day vulnerabilities

- Links to fake login pages for stealing credentials

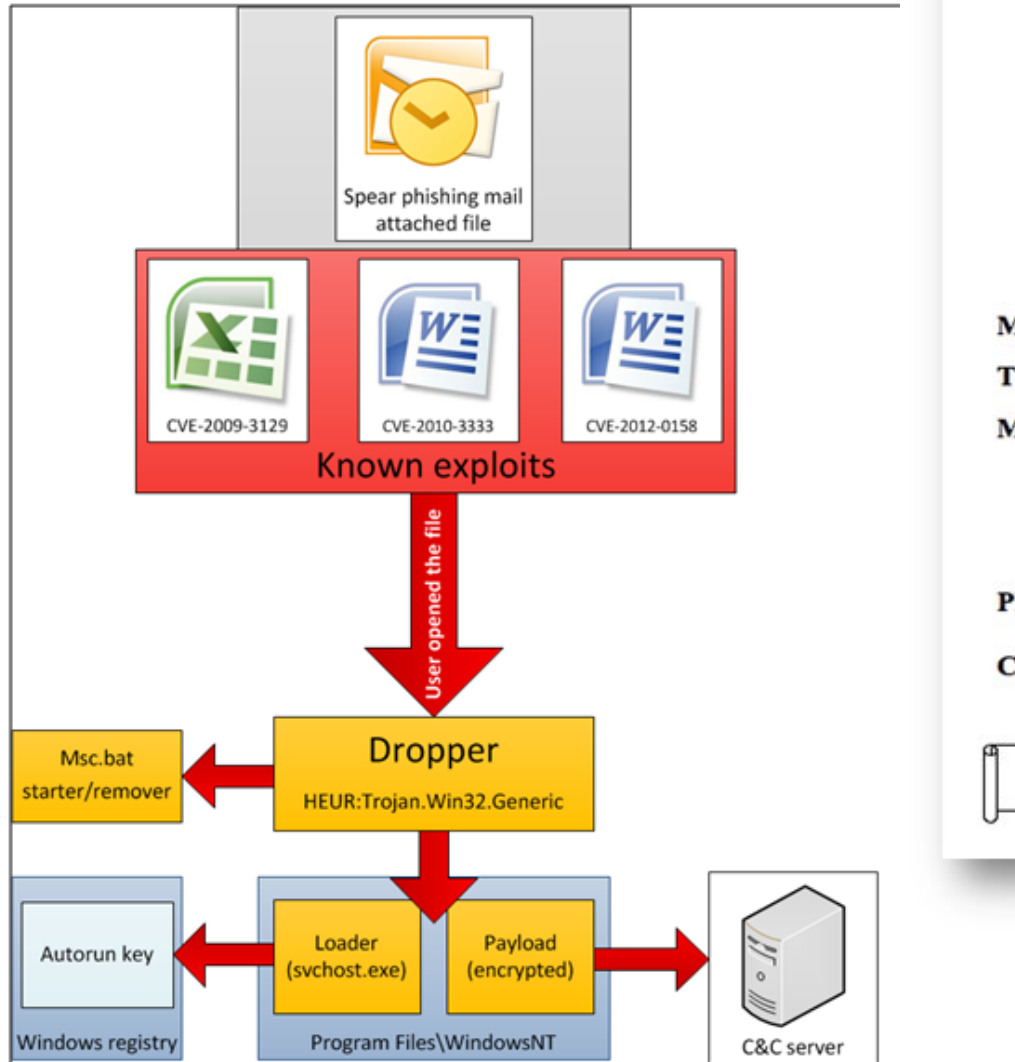
Numerous recent incidents

Operation "Red October"

Victims of advanced cyber-espionage network



Operation "Red October" (2012)



Diplomatic car for sale



MODEL: Mazda 323- 1998

DISPLACEMENT: 1800 cc

TRANSMISSION: Automatic

FUEL: Benzin

MILEAGE: 145.000 km

*Power Steering - Electric Windows - AM/FM Stereo -
Electric Mirrors - Air Conditioning - Remote central
locking with Alarm - Extra snow tires.*

PRICE: 2.700 \$ (USD)

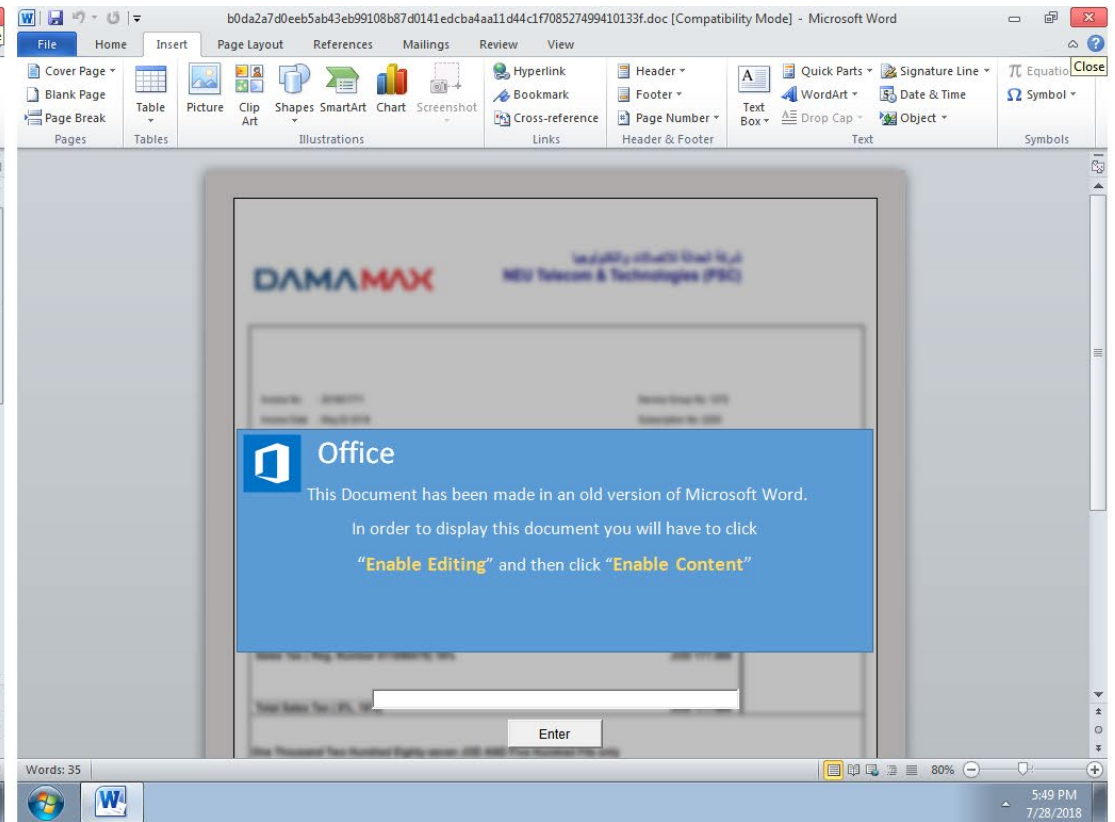
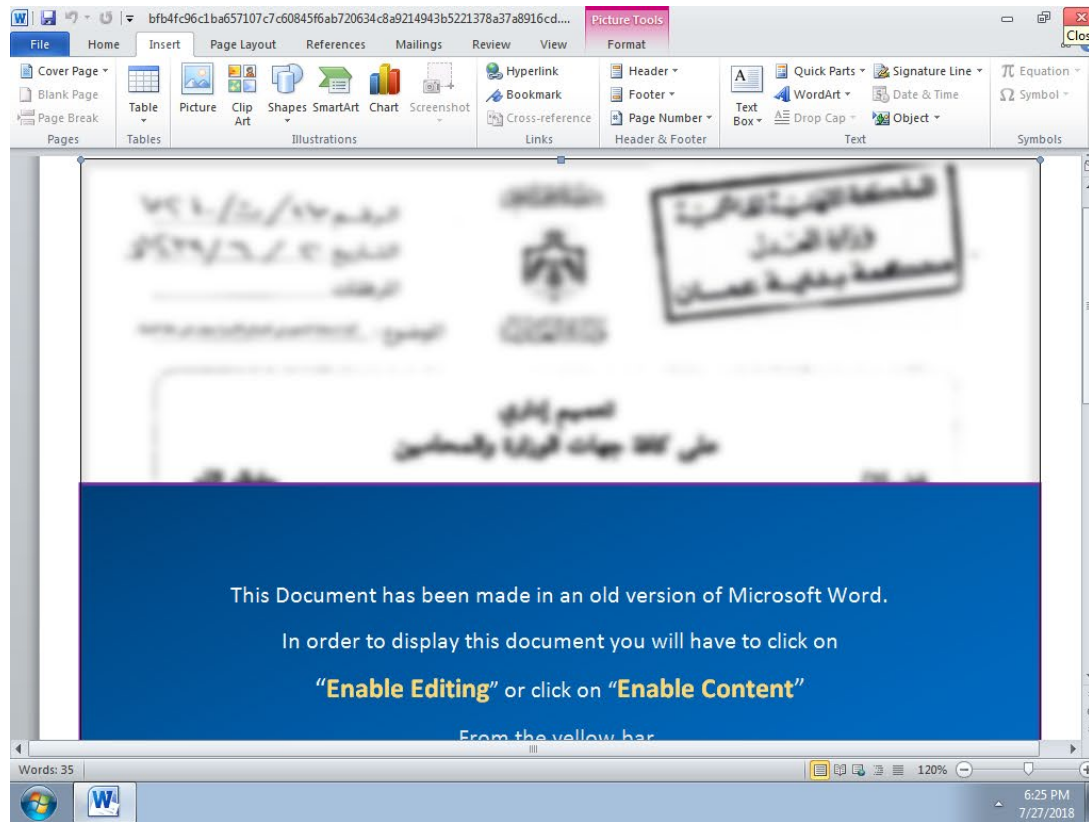
CONTACT: &&&&&&&&& - &&&&&&&&&&

THE CAR IS IN A VERY GOOD CONDITIONS

MuddyWater (2018)

Social engineering to enable macros

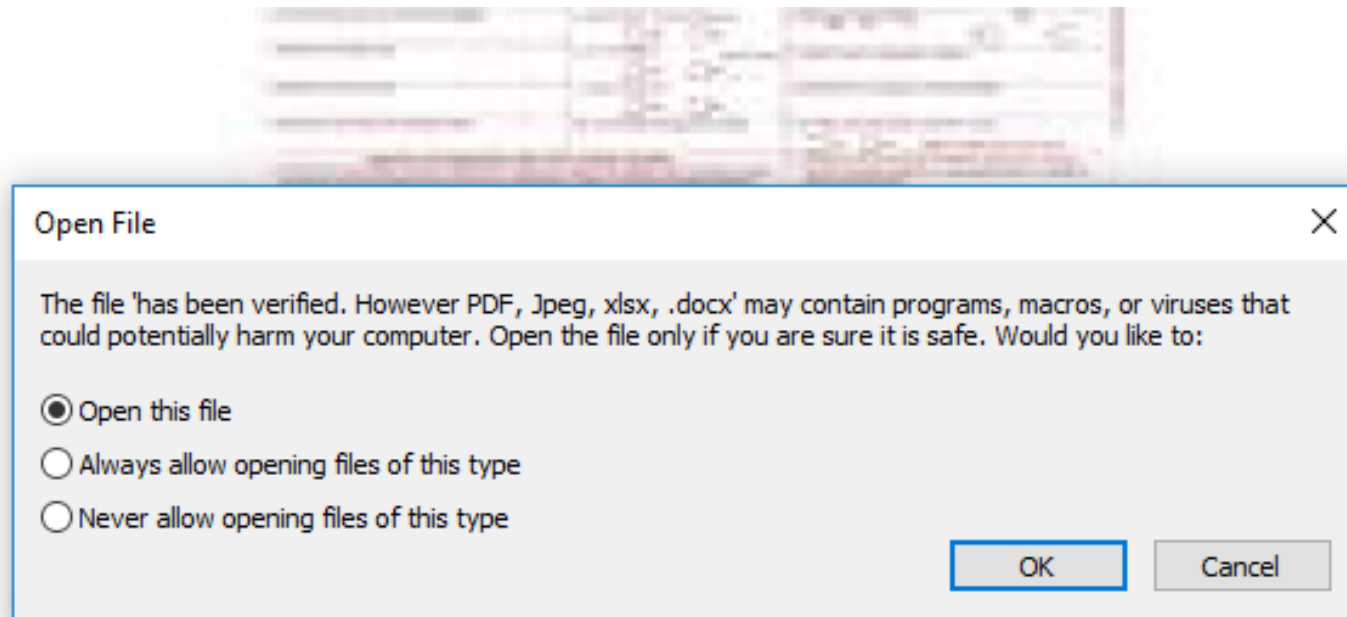
Decoy document images according to the target's country



Malicious PDF Campaign (2022)

“REMMITANCE INVOICE.pdf” sent as email attachment

After opening the document, Adobe Reader prompts the user to open a Word .docx file named “has been verified. However PDF, Jpeg, xlsx, .docx”



Business Email Compromise

Attacker uses email to trick someone into sending money or divulging confidential company info

Main differences from other email-based attacks

- Mostly text: no malware, malicious links, or attachments

- Target specific individuals within organization

- Carefully personalized to the intended victim based on extensive prior research

Common theme: ask for a fake bill to be paid

- Time sensitive, authoritative source (e.g., CEO, CFO), careful impersonation (writing style, trusted information), specific instructions, ...

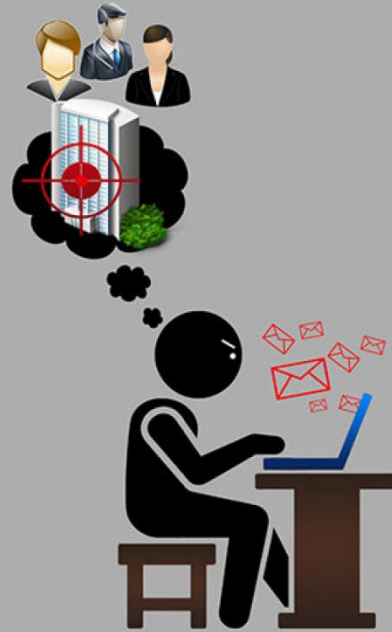
BEC scams are on the rise due to increased remote work

Step 1: Identifying a Target



Organized crime groups target businesses in the U.S. and abroad by exporting information available online to develop a profile on the company and its executives.

Step 2: Grooming



Spearphishing emails and/or phone calls target a victim company's officials (typically in the financial department).

Perpetrators use persuasion and pressure to manipulate and exploit employees' human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information



The victim is convinced they are conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer



Upon transfers, the funds are steered to a bank account control by the organized crime group.*



*Note: Perpetrators may continue to groom the victims into transferring more funds.

Business Email Compromise Timeline

An outline of how the business email compromise is executed by some organized crime groups

Personal example #1: Phishing message targeting SBU users

From: SBU Team <ebrahle2@kent.edu>
Date: Tue, Feb 2, 2016 at 8:42 PM
Subject: cyber security
To: XXXXXXXXXXXXX

We've detected spam-like activity in your webmail account, which is against our Acceptable Use Policy (AUP).

Kindly click on the link below to verify that you're the owner of the account and not a spammer.

<http://is.gd/stonybrooksecure>

We apologize for any inconvenience this may have cause you.

Thanks,
SBU Team

Personal (counter) example #2: *Legitimate* message from an IT department

From: XXXXXXXXXXXX
Date: XXXXXXXXXXXX
Subject: Important! You must change your XXXXXXXX password
To: XXXXXXXXXXXXXXXX

[This is not a spam mail, this email is from me, XXXXXXXXXXXXXXXX]

Member of XXXXXXXXXXXX Department,

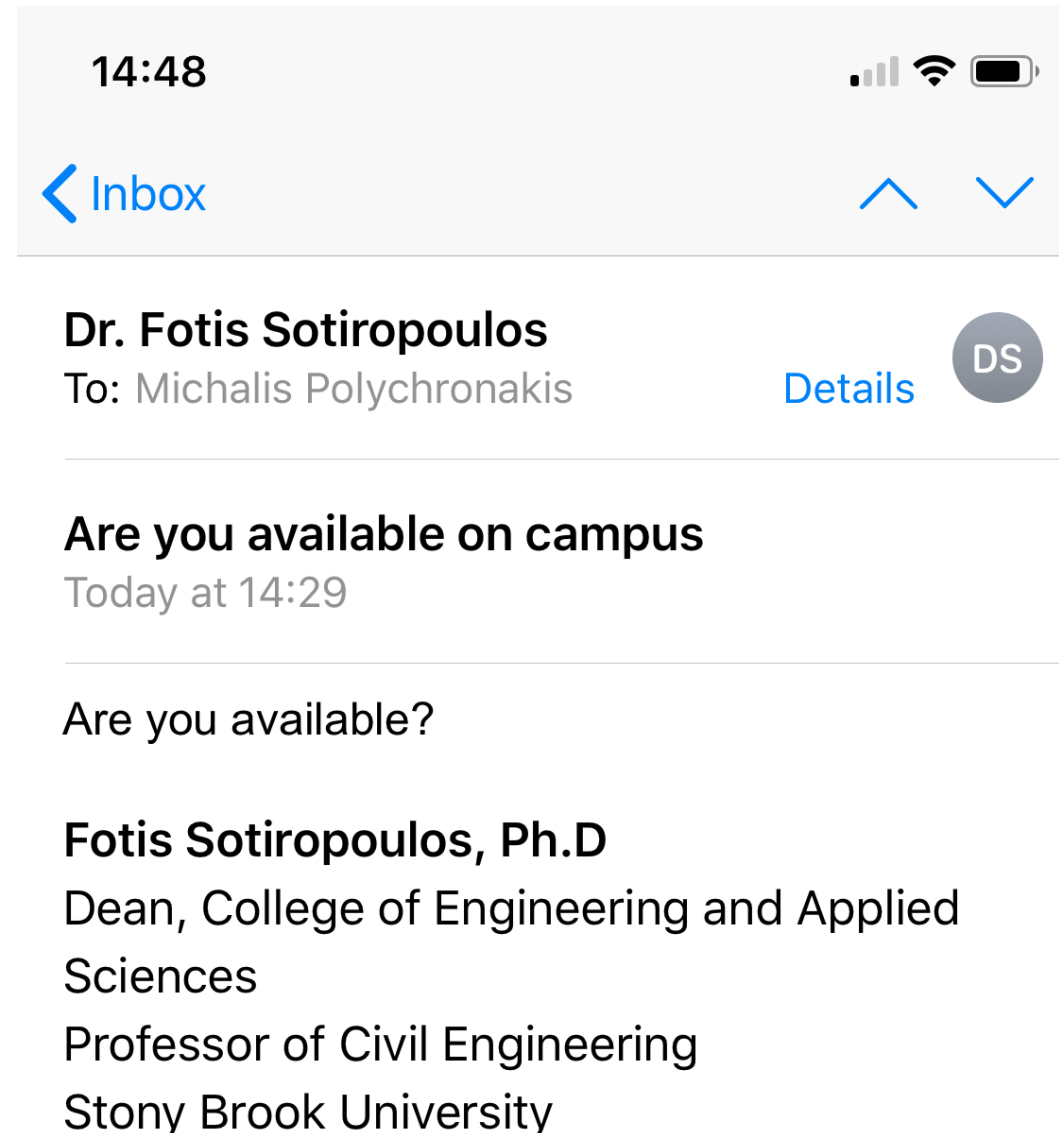
PLEASE CHANGE YOUR XXXXXXXX PASSWORD!

We just upgraded the security of XXXXXXXX. Your current password is no longer working. You must change your password if you want to log into XXXXXXXX. [...]

To change your XXXXXXXX password:

<http://XXXXXXXXXXXX.XXX> -> forgot your password -> follow the instructions

Personal example #3: targeted phishing message (which I opened on iPhone)





Are you available on campus >



Dr. Fotis Sotiropoulos <Fotis.Sotiropoulos.stonybrook.edu@outlook.com>
to me ▾

Jan 18, 2019, 2:29 PM



Be careful with this message

Dr. Fotis Sotiropoulos has never sent you messages using this email address. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.

Report phishing

Looks safe



Are you available?

Fotis Sotiropoulos, Ph.D
Dean, College of Engineering and Applied Sciences
Professor of Civil Engineering
Stony Brook University

Personal (counter) example #4: Legitimate message to SBU users



Stony Brook University | Division of Information Technology

On Wednesday, April 22nd, the security certificate for the WolfieNet-Secure wireless network will be updated. This certificate update is executed every few years in order to keep our network security up to date. With so many of our services relying on the network, it is clear how vital network security is. The process to update the certificate on all your wireless devices is very simple and just takes about 1 minute to complete. Please visit the WolfieNet-Secure wireless network and all other networks

What do I need to do?

- Simply visit <http://getwolfienet.com> and follow the steps to update the certificate on your wireless device. It is strongly recommended that you follow this procedure before Wednesday, April 22nd or you are likely to have connectivity issues when returning to campus.

Goes through various redirects, none of which involve a stonybrook.edu domain, asking to download and run an untrusted .exe

Personal example #5: phishing message targeting SBU CS members

The screenshot shows an email client interface. At the top, there is a navigation bar with icons for back, download, warning, delete, mail, clock, checkmark, folder, and a menu icon. On the right, it says "2 of 26" with left and right arrows. Below this, the email subject is "Schedule Changed" with a yellow "External" tag and an "Inbox x" tag. To the right are icons for print and share. The sender is "Payroll Office at CS [redacted]@northeastern.edu" with a blue profile picture icon and "to me" below it. The time is "7:41 AM (1 hour ago)" with a star, a reply icon, and a menu icon. The main body of the email says "Your payroll report is now available online." Below this is a white box with a blue link "View Report Here" and the text "Sign in with your Username and password to access." At the bottom of the email, it says "Payroll Office | CS", "...", and "[Message clipped] [View entire message](#)". At the very bottom are two buttons: "Reply" and "Forward". A red box with a red border is positioned over the sender's name, containing the text "Sent from a real person's (compromised) account". A red arrow points from this box to the sender's email address.



Department of Computer Science

HOME

ABOUT US

ADMISSIONS

PEOPLE

RESEARCH

PROGRAMS

GIVING

Log in

Request new password

Username *

Enter your SBU - Computer Science Department username.

Password *

Enter the password that accompanies your username.

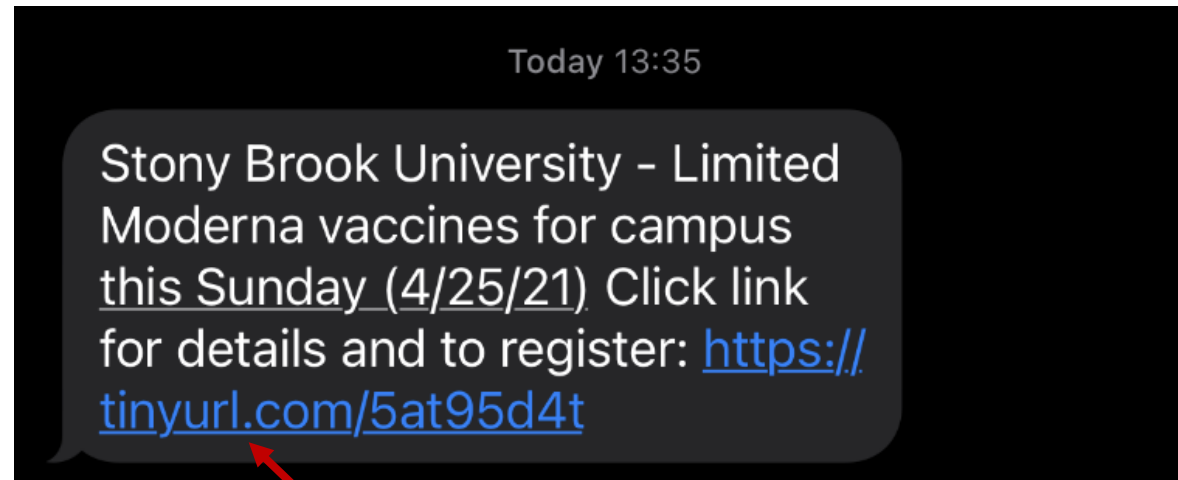
[Federated Log In](#)

Log in

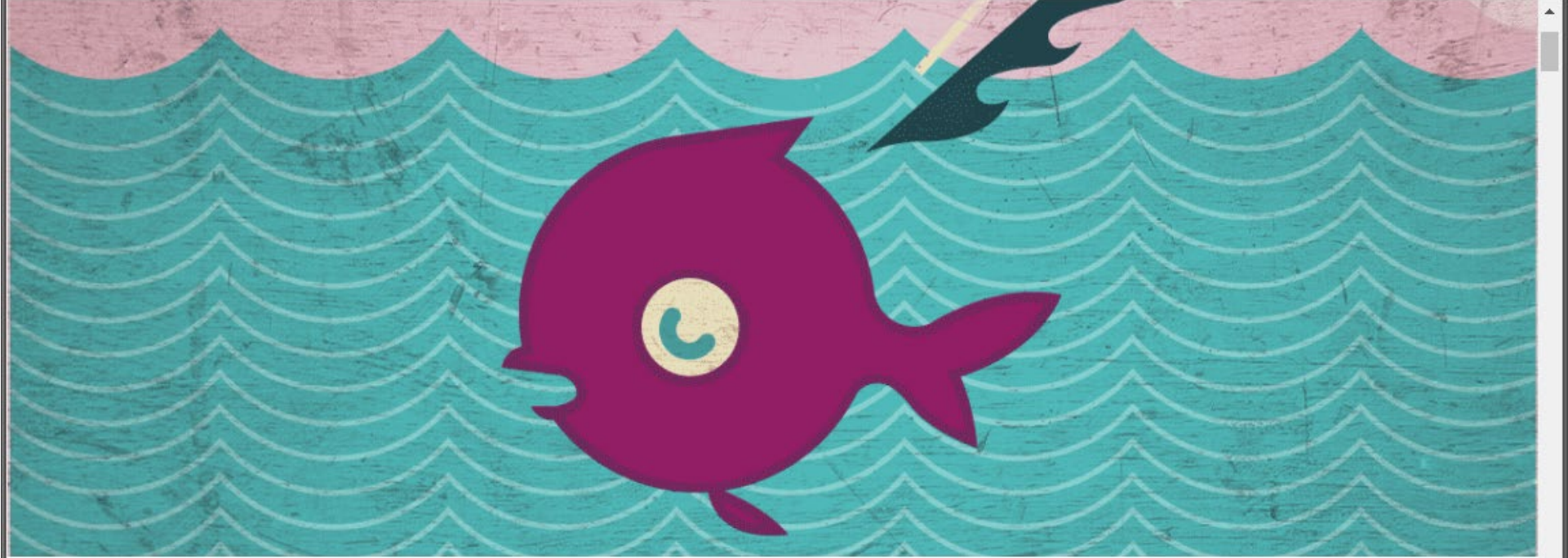
Department of Computer Science, Stony Brook University, Stony Brook, NY 11794-2424 631-632-8470 or 631-632-8471

[Stony Brook University Home Page](#) | [CEAS](#) | [Members Only Area](#)

Personal (counter) example #6: *Legitimate* SBU SMS



No idea what the actual target URL is



Phish For the Future

TECHNICAL ANALYSIS BY EVA GALPERIN AND COOPER QUINTIN | SEPTEMBER 27, 2017

This report describes “Phish For The Future,” an advanced persistent spearphishing campaign targeting digital civil liberties activists at [Free Press](#) and [Fight For the Future](#). Between July 7th and August 8th of 2017 we observed almost 70 spearphishing attempts against employees of internet freedom NGOs Fight for the Future and Free Press, all coming from the same attackers.

This campaign appears to have been aimed at stealing credentials for various business services including Google, Dropbox, and LinkedIn. At least one account was compromised and

Some of the attacks were generic, such as a link to view a Gmail document supposedly sent by a co-worker or a LinkedIn notification message from a colleague.

Another attack pretended to be from a target's husband, sharing family photos; the email was forged to include the husband's name.

Yet another attack pretended to be a YouTube comment for a real YouTube video that the target had uploaded.

Some of the headlines are designed to appeal to the political interests of the targets, such as: "George W. Bush ON TRUMP'S TWEET: A FREE PRESS IS 'INDISPENSABLE TO DEMOCRACY,""

The attackers sent emails titled "You have been successfully subscribed to Pornhub.com" and "You have been successfully subscribed to Redtube.com" to the victims. This was followed up minutes later with several emails all disguised as coming from Pornhub or Redtube with explicit subject lines. Each of the emails contained an unsubscribe link which directed the target to a Google credential phishing page.

From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: john.podesta@gmail.com
Subject: Someone has your password



Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:

Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

[CHANGE PASSWORD](#)

Best,
The Gmail Team

Gmail's filters didn't catch it...

```
00000000 3e 20 2a 46 72 6f 6d 3a 2a 20 47 6f 6f 67 6c 65 |> *From:* Google|
00000010 20 3c 6e 6f 2d 72 65 70 6c 79 40 61 63 63 6f 75 | <no-reply@accou|
00000020 6e 74 73 2e 67 6f 6f 67 6c 65 6d 61 69 6c 2e 63 | nts.googlemail.c|
00000030 6f 6d 3e 0d 0a 3e 20 2a 44 61 74 65 3a 2a 20 4d | om>..> *Date:* M|
00000040 61 72 63 68 20 31 39 2c 20 32 30 31 36 20 61 74 | arch 19, 2016 at|
00000050 20 34 3a 33 34 3a 33 30 20 41 4d 20 45 44 54 0d | 4:34:30 AM EDT.|
00000060 0a 3e 20 2a 54 6f 3a 2a 20 6a 6f 68 6e 2e 70 6f | .> *To:* john.po|
00000070 64 65 73 74 61 40 67 6d 61 69 6c 2e 63 6f 6d 0d | desta@gmail.com.|
00000080 0a 3e 20 2a 53 75 62 6a 65 63 74 3a 2a 20 2a 53 | .> *Subject:* *S|
00000090 d0 be 6d 65 d0 be 6e 65 20 68 61 73 20 79 6f 75 | ..me..ne has you|
000000a0 72 20 70 61 73 73 77 d0 be 72 64 2a 0d 0a 3e 0d | r passw..rd*..>.|
000000b0 0a 3e 20 53 d0 be 6d 65 d0 be 6e 65 20 68 61 73 | .> S..me..ne has|
000000c0 20 79 6f 75 72 20 70 61 73 73 77 d0 be 72 64 0d | your passw..rd.|
000000d0 0a 3e 20 48 69 20 4a 6f 68 6e 0d 0a 3e 0d 0a 3e | .> Hi John..>..>|
```


Sensibly, Podesta forwarded the email, asking what to do

From: Charles ██████████ <██████████@hillaryclinton.com>
Date: March 19, 2016 at 9:54:05 AM EDT
To: Sara ██████████ <██████████@hillaryclinton.com>, Shane ██████████
<██████████@hillaryclinton.com>
Subject: Re: Someone has your password

Sara,

This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: <https://myaccount.google.com/security> to do both. It is absolutely imperative that this is done ASAP.

If you or he has any questions, please reach out to me at 410.██████████.██████████

Campaign aide Charles Delavan told the NYT he knew the email was a phishing attack, given that the Clinton campaign was getting a steady stream of them. He meant to reply that the email was “illegitimate.”

The IT team did send a legitimate Google link, but that’s not the one Podesta clicked

How APT28/FANCYBEAR/GRU breached John Podesta's account



TOUR ENTERPRISE RESOURCES ABOUT

LOGIN

SIGN UP

MAR 19

http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?
e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D
&img=Ly9saDQuZ29vZ2xldXNlcmNvb3Rlc3RhbnRlbnQuY29tLy1RZVlPbHJkVWp2WS9BQUFBQUFBQUFB...
http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?
e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvb3Rlc3RhbnRlbnQuY29tLy1RZVlPbHJkVWp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT9CQldVOVQ0bUZUWS9waG90by5qcGc%3D&id=1sutlodlwe

bitly.com/ COPY

Decode from Base64 format

Simply use the form below

am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ

< DECODE >

UTF-8

(You may also select input charset.)

john.podesta@gmail.com

Link from database of 8,909 bitly links used by APT28/GRU in an expansive spear-phishing spree against 3,907 individual Gmail accounts.

Data harvested as a result of an API setting error on the part of APT28 by SecureWorks between October 2015 and May 2016.

@ridt

2 CLICKS

SEP 6 SEP 12 SEP 18

OCT 6 OCT 12

DATA IN UTC



This link has been flagged as redirecting to malicious or spam content.

MAR 19

<http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbhRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...>
[http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbhRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...<u>http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbhRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...</u>](http://myaccount.google.com-securitysettingpage.tk/security/signinoptions/password?e=am9obi5wb2Rlc3RhQGdtYWlsLmNvbQ%3D%3D&fn=Sm9obiBQb2Rlc3Rh&n=Sm9obg%3D%3D&img=Ly9saDQuZ29vZ2xldXNlcmNvbhRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...)

bitly.com/1PibSU0 COPY

Decode from Base64 format

Simply use the form below

Ly9saDQuZ29vZ2xldXNlcmNvbhRlbnQuY29tLy1RZVIPbHJkVGp2WS9BQUFBQUFBQUFBSS9BQUFBQUFBQUFBCT...

< DECODE > UTF-8 (You may also select input charset.)

//lh4.googleusercontent.com/-QeYOIrdTjvY/AAAAAAAAAAI/AAAAAAAAABM/BBWU9T4mFTY/photo.jpg

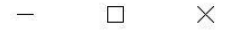
https://lh4.googleusercontent.com/-QeYOIrdTjvY/AAAAAAAAAAI/AAAAAAAAABM/BBWU9T4mFTY/photo.jpg



2 CLICKS



http://myaccount.google.com-securitysettingpage.tk/security/signin → Gmail



One account. All of Google.

Sign in to continue to Gmail



John Podesta

john.podesta@gmail.com

Sign in

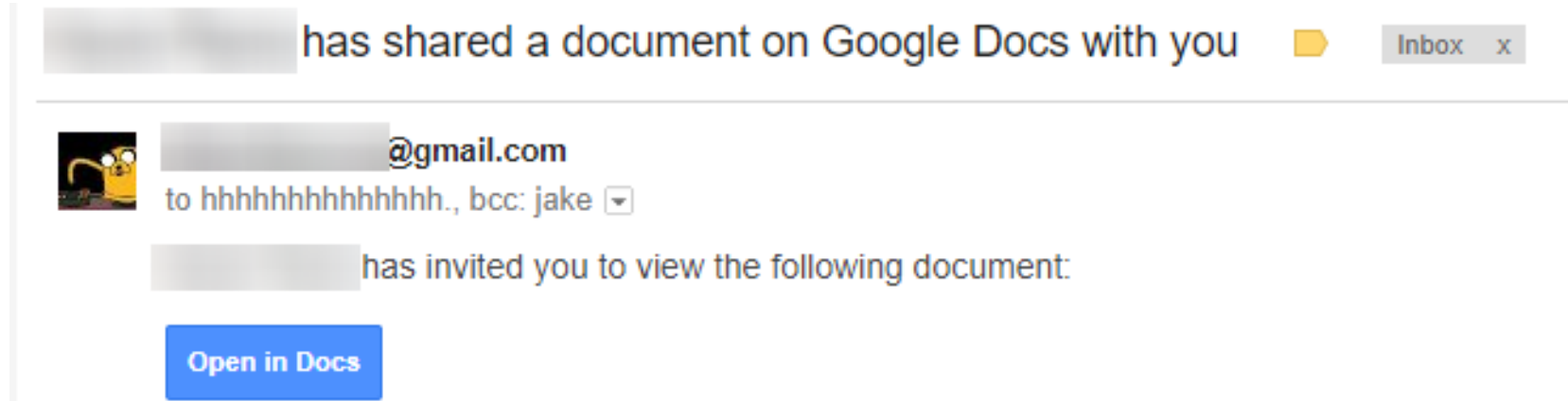
[Need help?](#)

[Sign in with a different account](#)

One Google Account for everything Google

Recent Google Docs Phishing Campaign

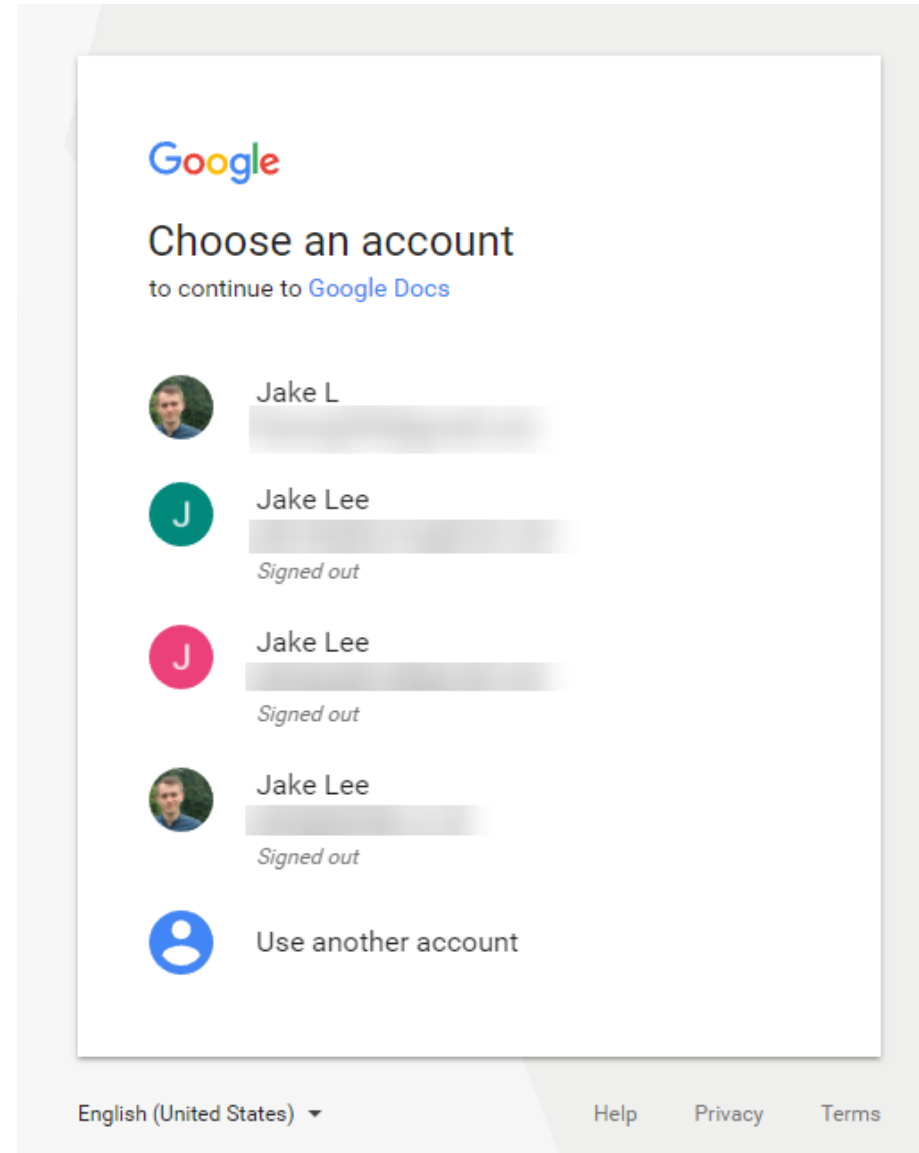
1) Fake "Google doc has been shared with you" email



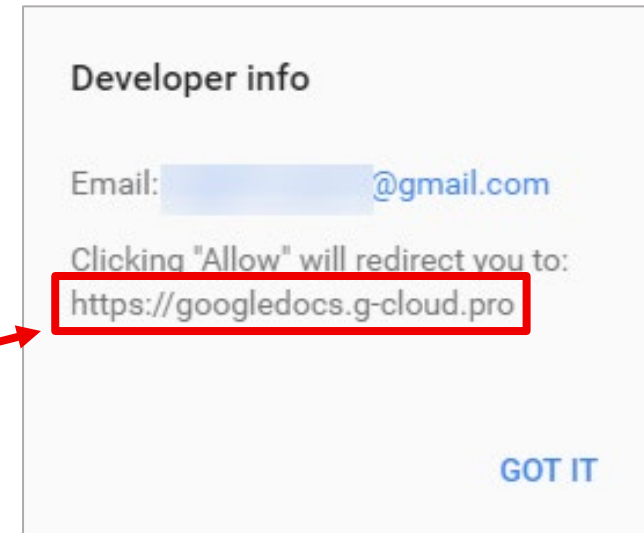
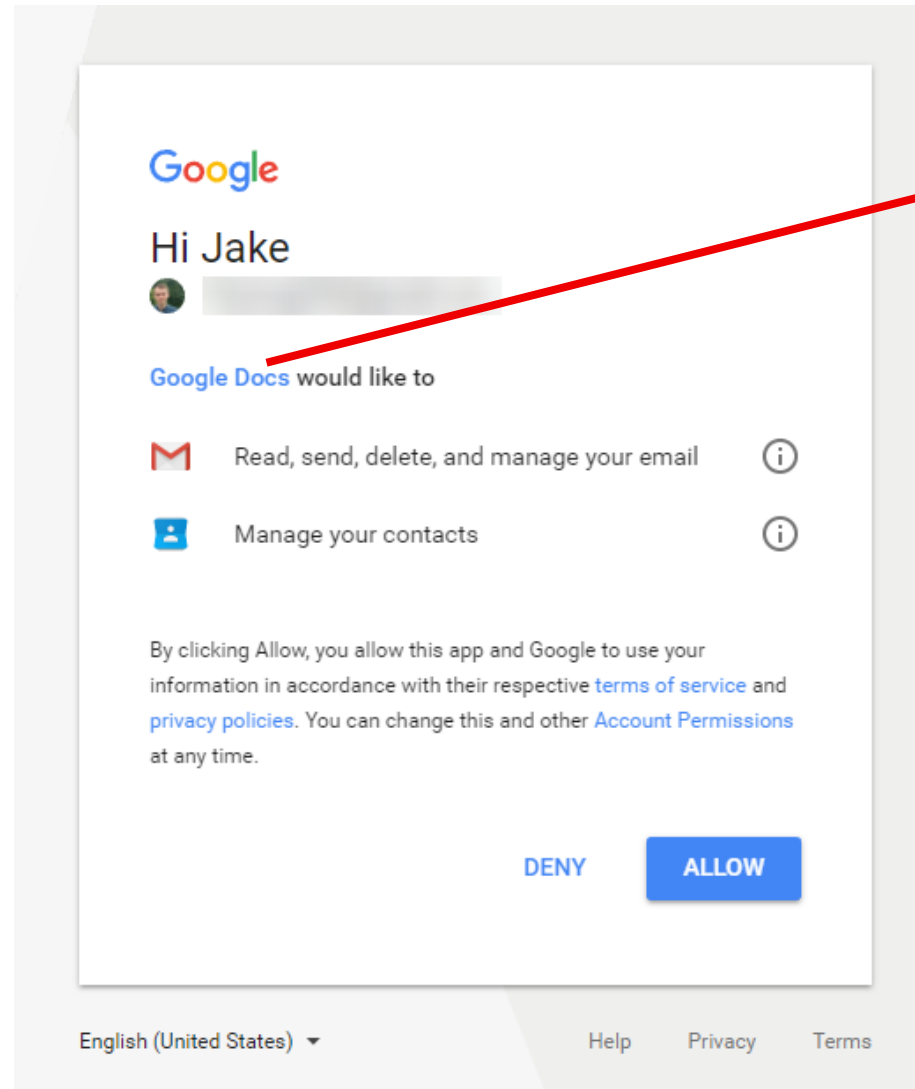
2) Button's URL looks legit

https://accounts.google.com/o/oauth2/auth?client_id=346348828325-vlpb3e70lp89pd823qrcb9jfsmu556t8.apps.googleusercontent.com&scope=

3) Real Google account selection prompt



4) "Google Docs would like to..."



TOP ^ **Twitter Investigation Report**SHARE   

SECTIONS

[Executive Summary](#)[Background](#)[Facts of the Hack](#)[A Visual Timeline](#)[DFS-Regulated
Cryptocurrency Companies
Respond](#)[Cybersecurity Weakness at
Twitter Contributed to
Hackers' Success](#)

Facts of the Hack

The Attackers Used Fraudulent Means to Access Twitter's Network and Internal Applications^[25]

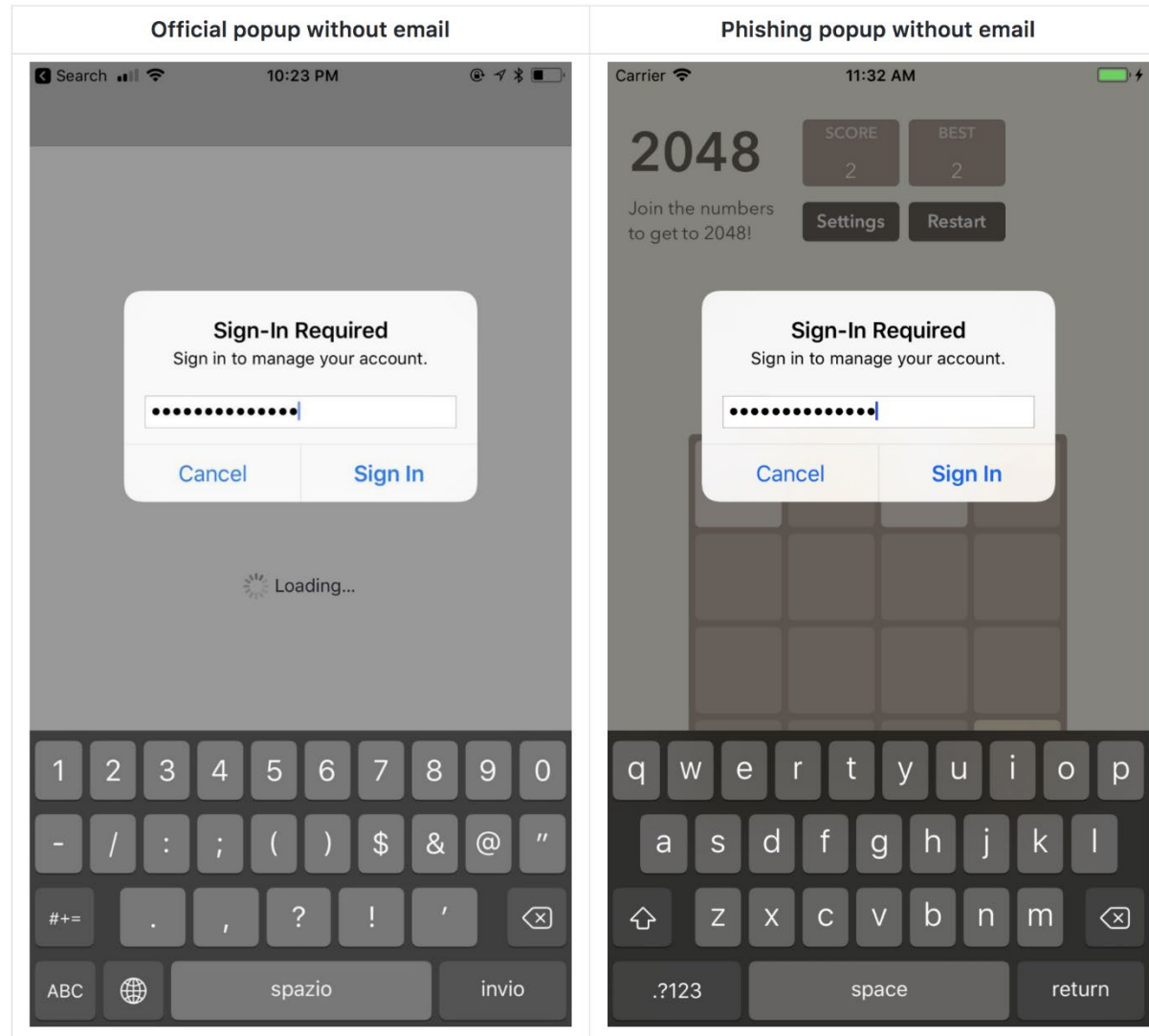
On July 14 and 15, 2020, the Hackers attacked Twitter.^[26] The Twitter Hack happened in three phases: (1) social engineering attacks to gain access to Twitter's network; (2) taking over accounts with desirable usernames (or "handles") and selling access to them; and (3) taking over dozens of high-profile Twitter accounts and trying to trick people into sending the Hackers bitcoin. All this happened in roughly 24 hours.

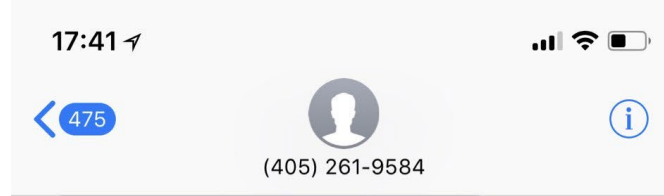
Phase One: Stealing Credentials through Social Engineering

The Twitter Hack started on the afternoon of July 14, 2020,^[27] when one or more Hackers called several Twitter employees and claimed to be calling from the Help Desk in Twitter's IT department. The Hackers claimed they were responding to a reported problem the employee was having with Twitter's Virtual Private Network ("VPN"). Since switching to remote working, VPN problems were common at Twitter. **The Hackers then tried to direct the employee to a phishing website that looked identical to the legitimate Twitter VPN website and was hosted by a similarly named domain.** As the employee entered their credentials into the phishing website, the Hackers would simultaneously enter the information into the real Twitter website. This false log-in generated an MFA notification requesting that the employees authenticate themselves, which some of the employees did.

The Department found no evidence the Twitter employees knowingly aided the Hackers. Rather, the Hackers used personal information about the employees to convince them that

Phishing beyond email





Did you request Google reset the password for todderick@gmail.com ? If not, respond with STOP.

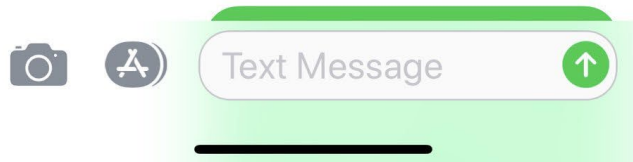
STOP

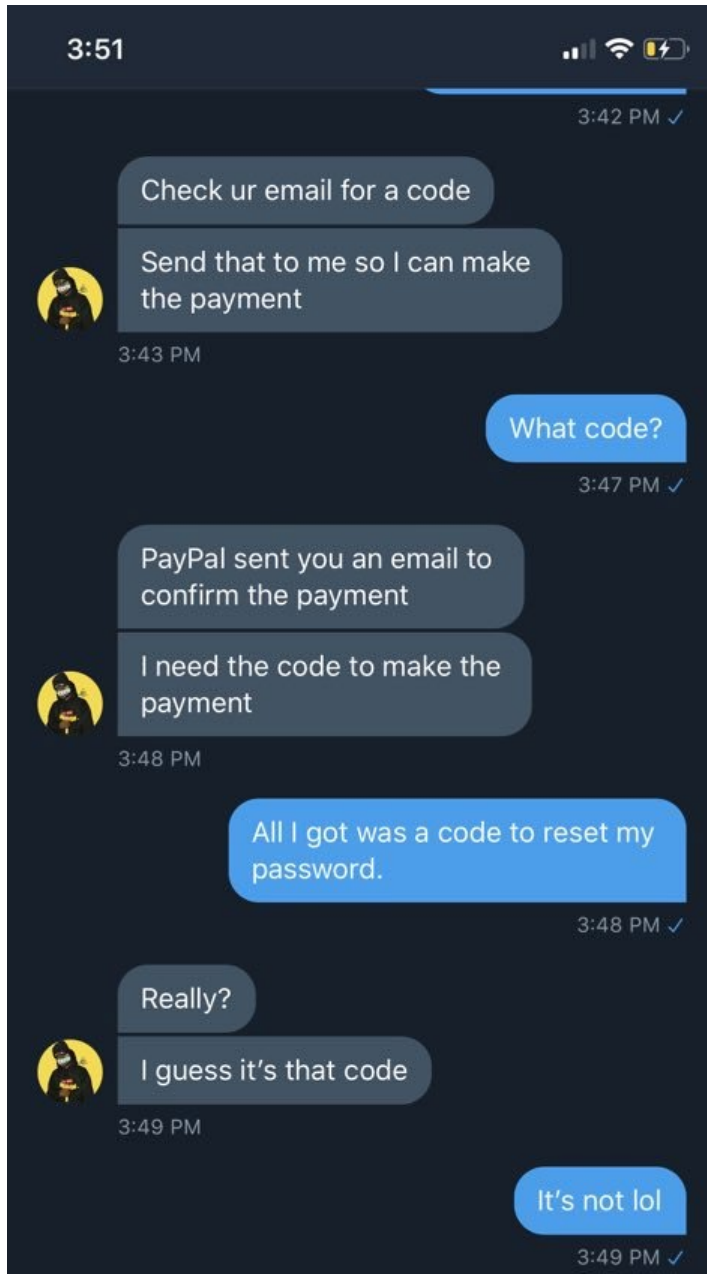
Confirm the 6 digit numerical code to STOP the password reset. Respond with "822" to have the verification code re-sent.

Clever

But no

Incorrect code. Confirm the 6 digit verification code to STOP the reset. Respond with "[822](#)" to have the verification code re-sent.





Text Message
Today 11:15 PM

On Feb02:Wells Fargo has temporarily blocked your account due to security website maintenance. Please sign in to verify your information: [https://\[REDACTED\]](https://[REDACTED])



BUSINESS

CULTURE

GEAR

IDEAS

SCIENCE

SECURITY

TRANSPORTATION

SHARE



MAT HONAN GEAR 08.06.12 08:01 PM

HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING



MOST POPULAR



CULTURE
'Jeopardy!' Legend Ken Jennings on James Holzhauer: 'It's Absolutel...
BRIAN BARRETT



SCIENCE
You're Not Getting Enough Sleep—and It's Killing You
EMILY DREYFUSS



BUSINESS
15 Months of Fresh Hell Inside Facebook
NICHOLAS THOMPSON, FRED VOGELSTEIN

➔ MORE STORIES

Google, Twitter, AppleID accounts compromised within one hour

Attacker remotely erased (!) all data on iPhone, iPad, and MacBook

Lost photos of his daughter that were not saved anywhere else ;-(

4:33pm – call to AppleCare

Caller reported that he couldn't get into their [me.com](#) email

The caller couldn't answer the security questions

Apparently, this happens quite often...

Apple representative asked an alternative set of questions

Billing address

Last four digits of credit card

The hackers had to find just those two pieces of information...

Step 0: Reconnaissance

Twitter account → personal website → personal Gmail address

Google's account password recovery page → no 2FA was used → page showed that reset confirmation has been sent to `m••••n@me.com` (me.com == Apple's free email)

`m••••n@me.com` is the backup email address → becomes attackers' **primary target**

Step 1: Find billing address

Whois search on website's domain

Step 2: Find last four digits of credit card on Apple account

Call Amazon: *"please add a new credit card to my account"* → Amazon asked for: name, e-mail address, billing address

Call Amazon (again): *"I've lost access to my account"* → provide name, billing address, (newly added) credit card number → Amazon allows you to add a new email to the account → password reset → view all ccards on file (last four digits – *good enough!*)

What else went wrong

No two-factor authentication

This was in 2012, awareness about 2FA was not that high

Daisy-chained accounts: Amazon → Apple ID → Gmail → Twitter

Same username across accounts

mhonan@gmail.com, mhonan@me.com, mhonan@wired.com

Find My Mac enabled for laptop

Perhaps not as useful as Find My Phone (phones are more likely to get lost)

Remote hard drive wipe → system asks to create a four-digit recovery PIN

If wipe is initiated by attacker, there's no way for the victim to know the PIN

No regular backups

Phishing Countermeasures

Stop confusing users! Organizations should not use URL shorteners etc.

User education

Don't trust links in emails – type the address in your browser

(analogous to: don't trust phone calls from your bank that ask for your info – ***always hang up and call the number at the back of your card***)

Augmenting password logins

Two-step login: show user-specific information before prompting for the password

Too inconvenient, easy to fool/ignore → not used anymore



Anti-phishing filters, detection tools, ...

~~2-factor authentication~~ → **U2F/FIDO**

Evilginx2 <https://github.com/kgretzky/evilginx2>

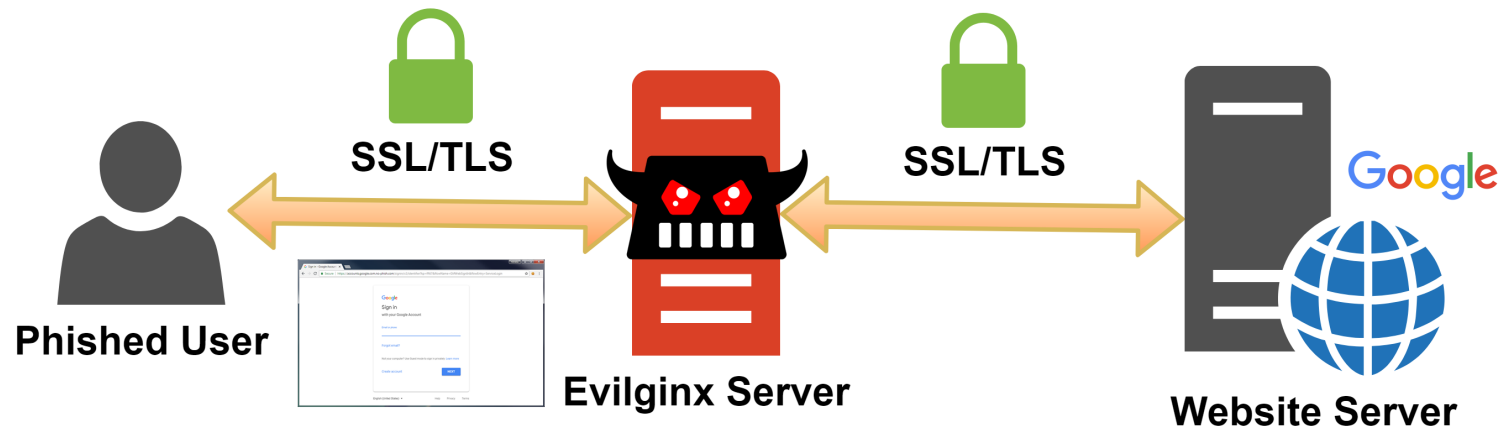
Man-in-the-middle attack framework for phishing login credentials along with session cookies

Bypasses 2-factor authentication

No need for HTML templates: just a web proxy

Victim's traffic is forwarded to the real website

TLS termination at the proxy (e.g., using a LetsEncrypt certificate)

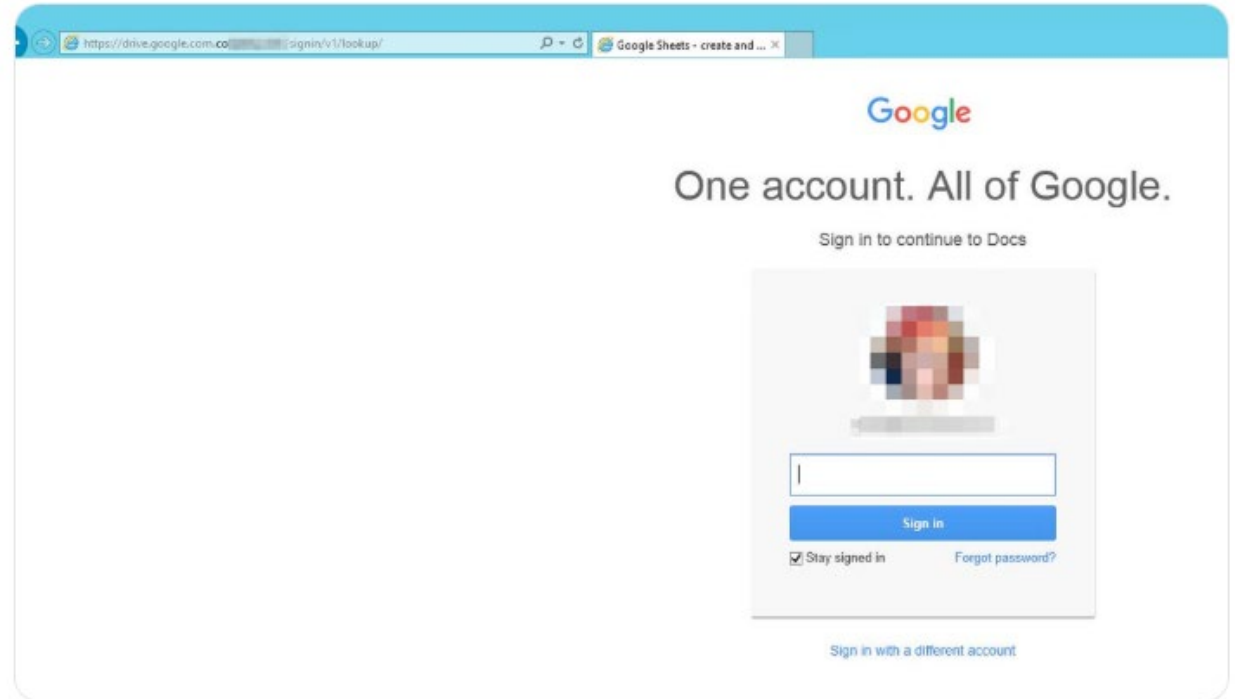




Justin Warner
@sixdub

Follow

I love digging through certificate transparency logs. Today, I saw a fake Google Drive landing page freshly registered with Let's Encrypt. It had a hardcoded picture/email of presumably the target. These can be a wealth of info that I recommend folks checking out.



5:21 PM - 22 Jul 2018

Evilginx2's Tokenized phishing URLs

Scanners look into public certificate transparency logs for newly registered domains

“For some phishing pages, it took usually one hour for the hostname to become banned and blacklisted by popular anti-spam filters”

Solution: create unique phishing URLs

Response to scanner: benign page

<https://totally.not.fake.linkedin.foo.com/auth/signin>

Response to victim: malicious page

https://totally.not.fake.linkedin.foo.com/auth/signin?tk=secret_token

Additional countermeasure: temporarily hide the phishing page

While submitting it to bit.ly, sending it through email, appearing on CT log, ...

Modlishka <https://github.com/drk1wi/Modlishka>

Phishing reverse proxy

Support for the majority of 2FA authentication schemes

No website templates

User credential harvesting (with context based on URL parameter passed identifiers)

Web panel with a summary of collected credentials and user session impersonation

```
>>>> "Modlishka" Piotr Duszynski @drk1wi - Reverse Proxy started <<<<

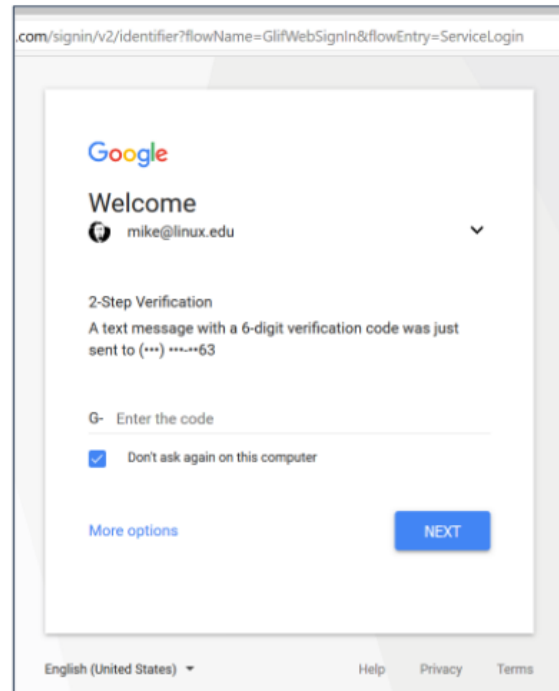
[127.0.0.1:443]
[127.0.0.1:443]

Listening on: [127.0.0.1:443]
Proxying [phishing.com.dev:443] via --> [https://google.com]
[Sat Dec 22 14:02:41 2018] INF Username collected ID:[42bc12cf-eea6-4cc1-acc9-84fe10b81f4c] username: phishingng
[Sat Dec 22 14:02:47 2018] INF Credentials collected ID:[42bc12cf-eea6-4cc1-acc9-84fe10b81f4c] username: phishingng password: supersecretpass
[Sat Dec 22 14:03:23 2018] INF [P] Tracking victim via initial parameter 9a0d22a9-19be-4c13-bc61-ff1dae2d7170
[Sat Dec 22 14:03:46 2018] INF Credentials collected ID:[9a0d22a9-19be-4c13-bc61-ff1dae2d7170] username: testuser password: yetanothersecretpass
```


CredSniper <https://github.com/ustayready/CredSniper>

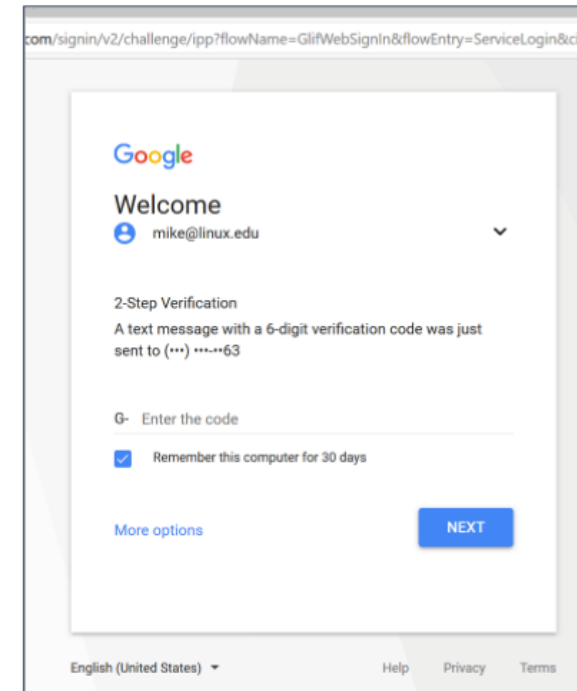
Exact login form clones for realistic phishing

Supports TLS via Let's Encrypt, and phishing 2FA tokens



Fake

**Real
Or
Fake?**




Real

Advanced Protection Program

https://landing.google.com/advancedprotection/

Google Advanced Protection Program Overview FAQ

Get started



Google's strongest security helps keep your private information safe.

The Advanced Protection Program safeguards users with high visibility and sensitive information, who are at risk of targeted online attacks. New protections are automatically added to defend against today's wide range of threats.

[Learn how to get started](#)