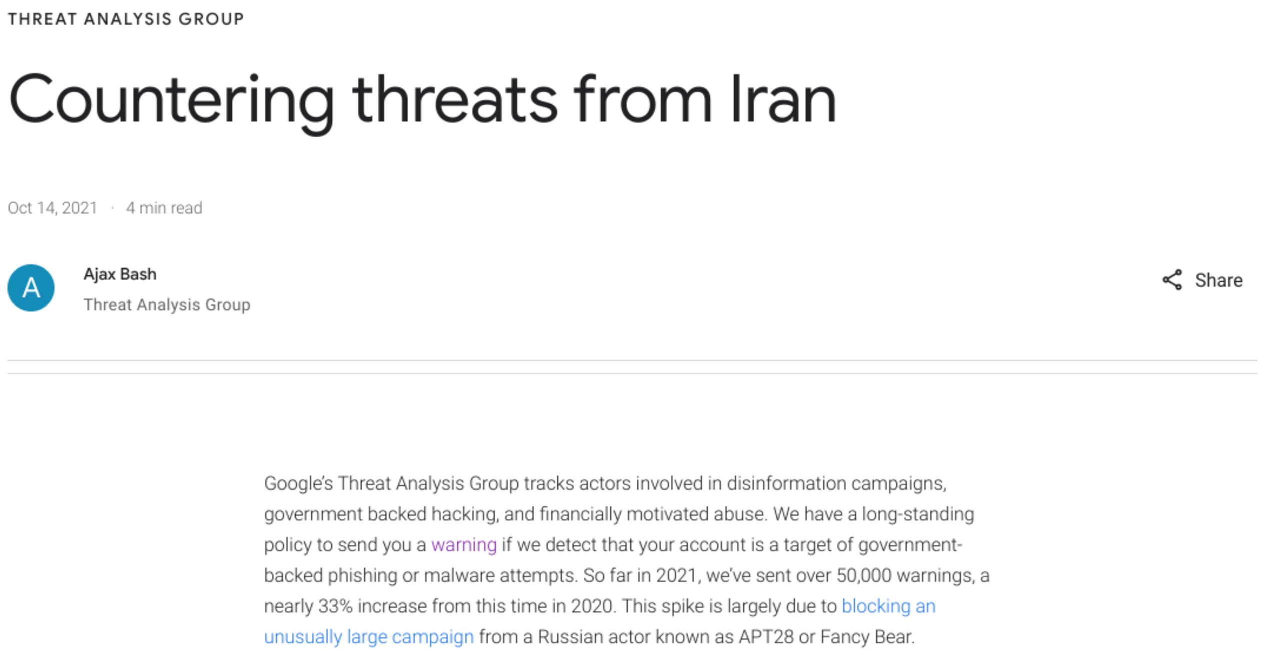
Countering threats from Iran

blog.google/threat-analysis-group/countering-threats-iran/

Ajax Bash

October 14, 2021



THREAT ANALYSIS GROUP

Countering threats from Iran

Oct 14, 2021 · 4 min read

Ajax Bash
Threat Analysis Group

Google's Threat Analysis Group tracks actors involved in disinformation campaigns, government backed hacking, and financially motivated abuse. We have a long-standing policy to send you a warning if we detect that your account is a target of government-backed phishing or malware attempts. So far in 2021, we've sent over 50,000 warnings, a nearly 33% increase from this time in 2020. This spike is largely due to blocking an unusually large campaign from a Russian actor known as APT28 or Fancy Bear.

Google's Threat Analysis Group tracks actors involved in disinformation campaigns, government backed hacking, and financially motivated abuse. We have a long-standing policy to send you a warning if we detect that your account is a target of government-backed phishing or malware attempts. So far in 2021, we've sent over 50,000 warnings, a nearly 33% increase from this time in 2020. This spike is largely due to blocking an unusually large campaign from a Russian actor known as APT28 or Fancy Bear.

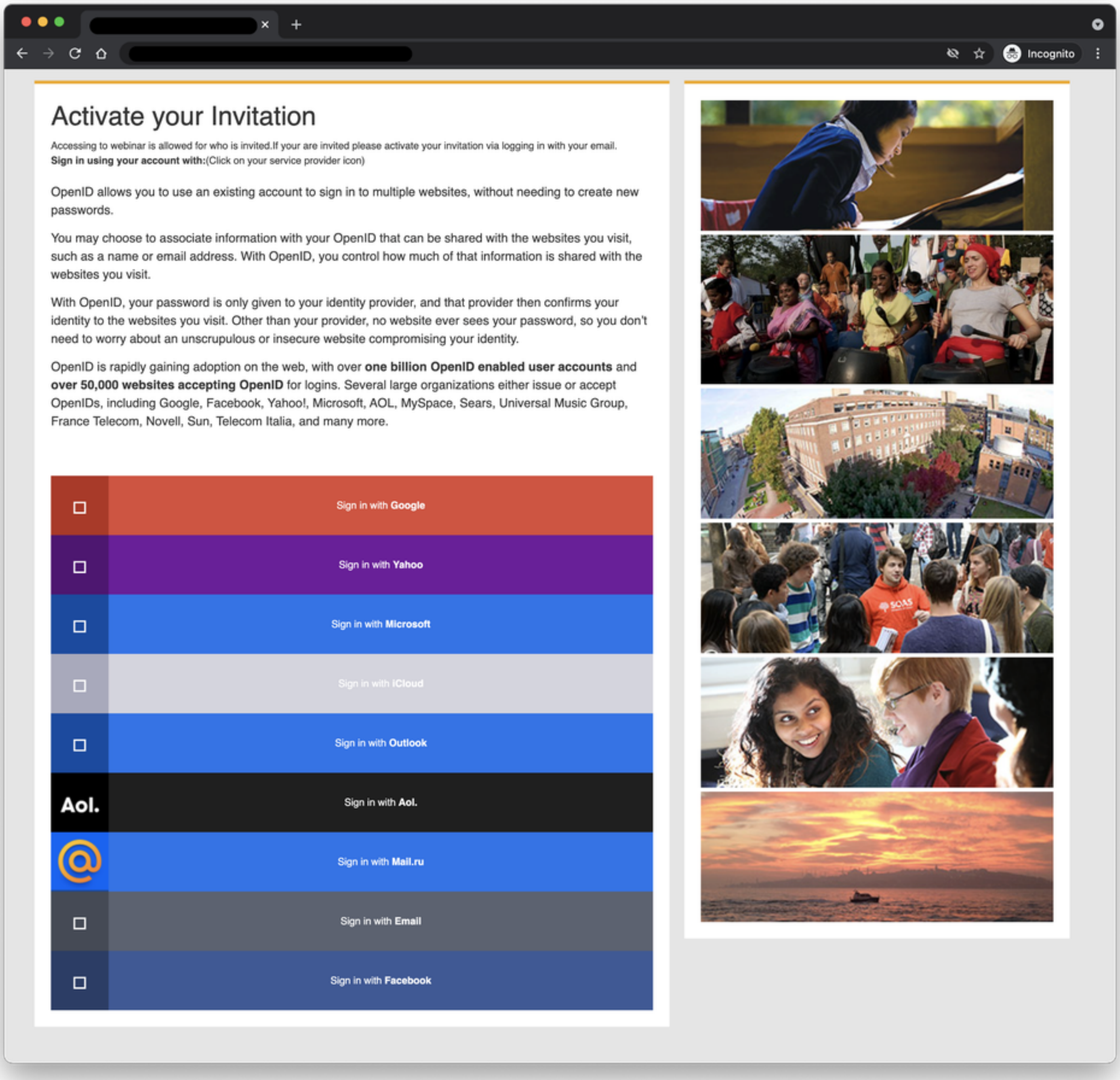
We intentionally send these warnings in batches to all users who may be at risk, rather than at the moment we detect the threat itself, so that attackers cannot track our defense strategies. On any given day, TAG is tracking more than 270 targeted or government-backed attacker groups from more than 50 countries. This means that there is typically more than one threat actor behind the warnings.

In this blog, we explore some of the most notable campaigns we've disrupted this year from a different government-backed attacker: APT35, an Iranian group, which regularly conducts phishing campaigns targeting high risk users. This is the one of the groups we disrupted during the 2020 US election cycle for its targeting of campaign staffers. For years, this group has hijacked accounts, deployed malware, and used novel techniques to conduct espionage aligned with the interests of the Iranian government.

Hijacked websites used for credential phishing attacks

In early 2021, APT35 compromised a website affiliated with a UK university to host a phishing kit. Attackers sent email messages with links to this website to harvest credentials for platforms such as Gmail, Hotmail, and Yahoo. Users were instructed to activate an invitation to a (fake) webinar by logging in. The phishing kit will also ask for second-factor authentication codes sent to devices.

APT35 has relied on this technique since 2017 — targeting high-value accounts in government, academia, journalism, NGOs, foreign policy, and national security. Credential phishing through a compromised website demonstrates these attackers will go to great lengths to appear legitimate – as they know it's difficult for users to detect this kind of attack.



[redacted]

[redacted]

Activate your Invitation

Accessing to webinar is allowed for who is invited.If your are invited please activate your invitation via logging in with your email.
Sign in using your account with:(Click on your service provider icon)

OpenID allows you to use an existing account to sign in to multiple websites, without needing to create new passwords.

You may choose to associate information with your OpenID that can be shared with the websites you visit, such as a name or email address. With OpenID, you control how much of that information is shared with the websites you visit.

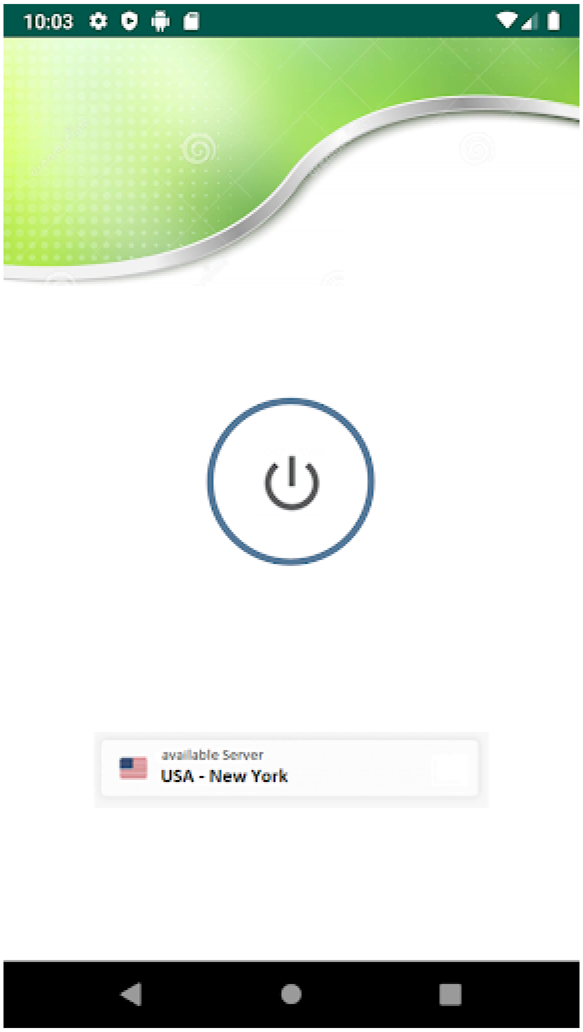
With OpenID, your password is only given to your identity provider, and that provider then confirms your identity to the websites you visit. Other than your provider, no website ever sees your password, so you don't need to worry about an unscrupulous or insecure website compromising your identity.

OpenID is rapidly gaining adoption on the web, with over **one billion OpenID enabled user accounts** and **over 50,000 websites accepting OpenID** for logins. Several large organizations either issue or accept OpenIDs, including Google, Facebook, Yahoo!, Microsoft, AOL, MySpace, Sears, Universal Music Group, France Telecom, Novell, Sun, Telecom Italia, and many more.

Phishing page hosted on a compromised website

Utilization of Spyware Apps

In May 2020, we discovered that APT35 attempted to upload spyware to the Google Play Store. The app was disguised as VPN software that, if installed, could steal sensitive information such as call logs, text messages, contacts, and location data from devices. Google detected the app quickly and removed it from the Play Store before any users had a chance to install it. Although Play Store users were protected, we are highlighting the app here as TAG has seen APT35 attempt to distribute this spyware on other platforms as recently as July 2021.



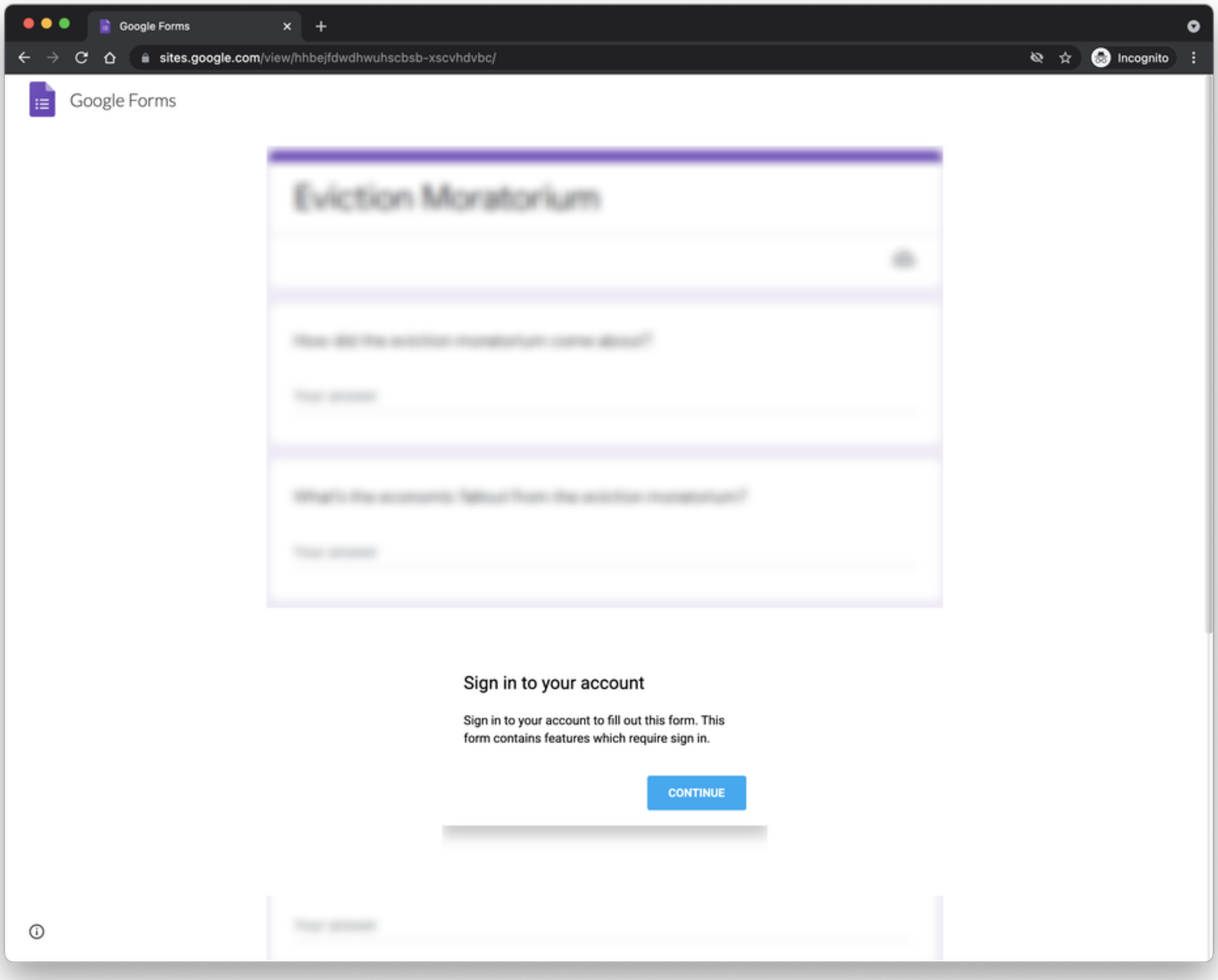
Spyware app disguised as a VPN utility

Conference-themed phishing emails

One of the most notable characteristics of APT35 is their impersonation of conference officials to conduct phishing attacks. Attackers used the Munich Security and the Think-20 (T20) Italy conferences as lures in non-malicious first contact email messages to get users to respond. When they did, attackers sent them phishing links in follow-on correspondence.

Targets typically had to navigate through at least one redirect before landing on a phishing domain. Link shorteners and click trackers are heavily used for this purpose, and are oftentimes embedded within PDF files. We've disrupted attacks using Google Drive, App

Scripts, and Sites pages in these campaigns as APT35 tries to get around our defenses. Services from Dropbox and Microsoft are also abused.



Eviction Moratorium

How did the eviction moratorium come about?

Your answer

What's the economic fallout from the eviction moratorium?

Your answer

Sign in to your account

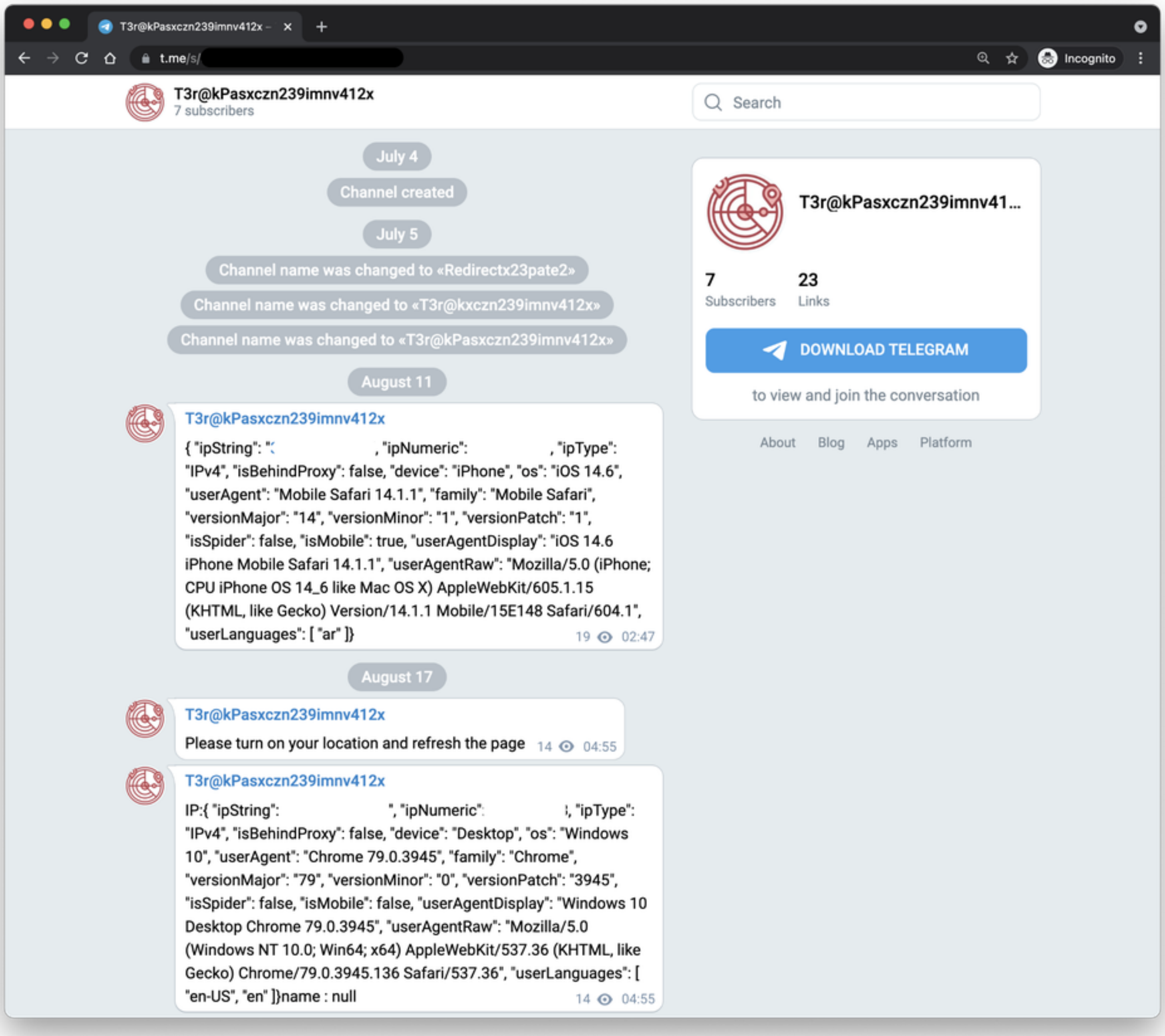
Sign in to your account to fill out this form. This form contains features which require sign in.

Your answer

Google Sites page disguised as a Google Form to redirect to a phishing site

Telegram for threat actor notifications

One of APT35's novel techniques involves using Telegram for operator notifications. The attackers embed javascript into phishing pages that notify them when the page has been loaded. To send the notification, they use the Telegram API sendMessage function, which lets anyone use a Telegram bot to send a message to a public channel. The attackers use this function to relay device-based data to the channel, so they can see details such as the IP, useragent, and locales of visitors to their phishing sites in real-time. We reported the bot to Telegram and they have taken action to remove it.



July 4

Channel created

July 5

Channel name was changed to «Redirectx23pate2»

Channel name was changed to «T3r@kxczn239imnv412x»

Channel name was changed to «T3r@kPasxczn239imnv412x»

August 11

T3r@kPasxczn239imnv412x

```
{ "ipString": "                    , "ipNumeric":                    , "ipType":
"IPv4", "isBehindProxy": false, "device": "iPhone", "os": "iOS 14.6",
"userAgent": "Mobile Safari 14.1.1", "family": "Mobile Safari",
"versionMajor": "14", "versionMinor": "1", "versionPatch": "1",
"isSpider": false, "isMobile": true, "userAgentDisplay": "iOS 14.6
iPhone Mobile Safari 14.1.1", "userAgentRaw": "Mozilla/5.0 (iPhone;
CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15
(KHTML, like Gecko) Version/14.1.1 Mobile/15E148 Safari/604.1",
"userLanguages": [ "ar" ]}
```

19 02:47

August 17

T3r@kPasxczn239imnv412x

Please turn on your location and refresh the page 14 04:55

T3r@kPasxczn239imnv412x

```
IP:{ "ipString":                    ", "ipNumeric":                    , "ipType":
"IPv4", "isBehindProxy": false, "device": "Desktop", "os": "Windows
10", "userAgent": "Chrome 79.0.3945", "family": "Chrome",
"versionMajor": "79", "versionMinor": "0", "versionPatch": "3945",
"isSpider": false, "isMobile": false, "userAgentDisplay": "Windows 10
Desktop Chrome 79.0.3945", "userAgentRaw": "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/79.0.3945.136 Safari/537.36", "userLanguages": [
"en-US", "en" ]}name : null
```

14 04:55

Public Telegram channel used for attacker notifications

How we keep users safe from these threats

We warn users when we suspect a government-backed threat like APT35 is targeting them. Thousands of these warnings are sent every month, even in cases where the corresponding attack is blocked. If you receive a warning it does not mean your account has been compromised, it means you have been identified as a target.

Workspace administrators are also notified regarding targeted accounts in their domain. Users are encouraged to take these warnings seriously and consider enrolling in the Advanced Protection Program or enabling two-factor authentication if they haven't already.

We also block malicious domains using Google Safe Browsing – a service that Google's security team built to identify unsafe websites across the web and notify users and website owners of potential harm. When a user of a Safe Browsing-enabled browser or app attempts to access unsafe content on the web, they'll see a warning page explaining that the content they're trying to access may be harmful. When a site identified by Safe Browsing as harmful appears in Google Search results, we show a warning next to it in the results.

Threat Analysis Group will continue to identify bad actors and share relevant information with others in the industry, with the goal of bringing awareness to these issues, protecting you and fighting bad actors to prevent future attacks.

Technical Details

Indicators from APT28 phishing campaign:

service-reset-password-moderate-digital.rf[.]gd

reset-service-identity-mail.42web[.]io

digital-email-software.great-site[.]net

Indicators from APT35 campaigns:

Abused Google Properties:

https://sites.google[.]com/view/ty85yt8tg8-download-rtih4ithr/

https://sites.google[.]com/view/user-id-568245/

https://sites.google[.]com/view/hhbejfdwdhwuhscbsb-xscvhdvbc/

Abused Dropbox Properties:

https://www.dropbox[.]com/s/68y4vpfu8pc3imf/Iraq&Jewish.pdf

Phishing Domains:

nco2[.]live

summit-files[.]com

filetransfer[.]club

continuetogo[.]me

accessverification[.]online

customers-verification-identifier[.]site

service-activity-session[.]online

identifier-service-review[.]site

recovery-activity-identification[.]site

review-session-confirmation[.]site

recovery-service-activity[.]site

verify-service-activity[.]site

service-manager-notifications[.]info

Android App:

https://www.virustotal.com/gui/file/5d3ff202f20af915863eee45916412a271bae1ea3a0e20988309c16723ce4da5/detection

Android App C2:

communication-shield[.]site

cdsa[.]xyz

POSTED IN:

Threat Analysis Group