Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media

proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists

July 11, 2022

Blog

Threat Insight

Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media

July 14, 2022 Crista Giering, Joshua Miller, Michael Raggi and the Proofpoint Threat Research Team

Key Takeaways

- Those involved in media make for appealing targets given the unique access, information, and insights they can provide on topics of state-designated import.
- Proofpoint researchers have observed APT actors since early 2021 regularly targeting and posing as journalists and media organizations to advance their state-aligned collection requirements and initiatives.
- The identified campaigns have leveraged a variety of techniques from using web beacons for reconnaissance to sending malware to establish initial access into the target's network.
- The focus on media by APTs is unlikely to ever wane, making it important for journalists to protect themselves, their sources, and the integrity of their information by ensuring they have an accurate threat model and secure themselves appropriately.

Overview

Journalists and media organizations suffer from many of the same threats as everyone else. Between threat actors wanting to steal credentials to resell or to utilize compromised hosts for brokered initial access to spread ransomware, among other threats, this sector is no stranger to the dangers of the threat landscape. Advanced persistent threat (APT) actors, however, look to those in the field of media for different purposes; ones that could have far-reaching impacts.

Journalists and media organizations are well sought-after targets with Proofpoint researchers observing APT actors, specifically those that are state-sponsored or state-aligned, routinely masquerading as or targeting journalists and media organizations because of the unique access and information they can provide. The media sector and those that work within it can open doors that others cannot. A well-timed, successful attack on a journalist's email account could provide insights into sensitive, budding stories and source identification. A compromised account could be used to spread disinformation or pro-state propaganda, provide disinformation during times of war or pandemic, or be used to influence a politically charged atmosphere. Most commonly, phishing attacks targeting journalists are used for espionage or to gain key insights into the inner workings of another government, company, or other area of state-designated import.

Proofpoint data since early 2021 shows a sustained effort by APT actors worldwide attempting to target or leverage journalists and media personas in a variety of campaigns, including those well-timed to sensitive political events in the United States. Some campaigns have targeted the media for a competitive intelligence edge while others have targeted journalists immediately following their coverage painting a regime in a poor light or as a means to spread disinformation or propaganda. For the purposes of this report, we focus on the activities of a handful of APT actors assessed to be aligned with the state interests of China, North Korea, Iran, and Turkey.

Targeting Journalists' Work Email Accounts

As observed in Proofpoint data, targeting journalists' work email accounts is by far the most seen locus of attack used by APT actors against this target set. It is important to note that journalists are communicating with external, foreign, and often semi-anonymous parties to gather information. This outreach increases the risk of phishing since journalists, often by necessity, communicate with unknown recipients more so than the average user. Verifying or gaining access to such accounts can be an entry point for threat actors for later stage attacks on a media organization's network or to gain access to desired information.

China

Since early 2021, the APT actor tracked by Proofpoint as **TA412**, known also as Zirconium based on public reporting by Microsoft about a phishing reconnaissance team within this larger APT threat actor designation, has engaged in numerous reconnaissance phishing campaigns targeting US-based journalists. TA412, which is believed to be aligned with the Chinese state interest and to have strategic espionage objectives, has favored using malicious emails containing web beacons in these campaigns. This is a technique consistently used by the threat actor since at least 2016, however, it was likely in use for years prior. Web beacons, which are commonly referred to as tracking pixels, tracking beacons, and web bugs, embed a hyperlinked non-visible object within the body of an email that, when enabled, attempts to retrieve a benign image file from an actor-controlled server.

Proofpoint researchers assess these campaigns have been intended to validate targeted emails are active and to gain fundamental information about the recipients' network environments. Web beacons can provide the following technical artifacts to an attacker which, in turn, can serve as reconnaissance information as a threat actor plans their next stage of attack:

- Externally visible IP addresses
- User-Agent string
- Email address
- Validation that the targeted user account is active

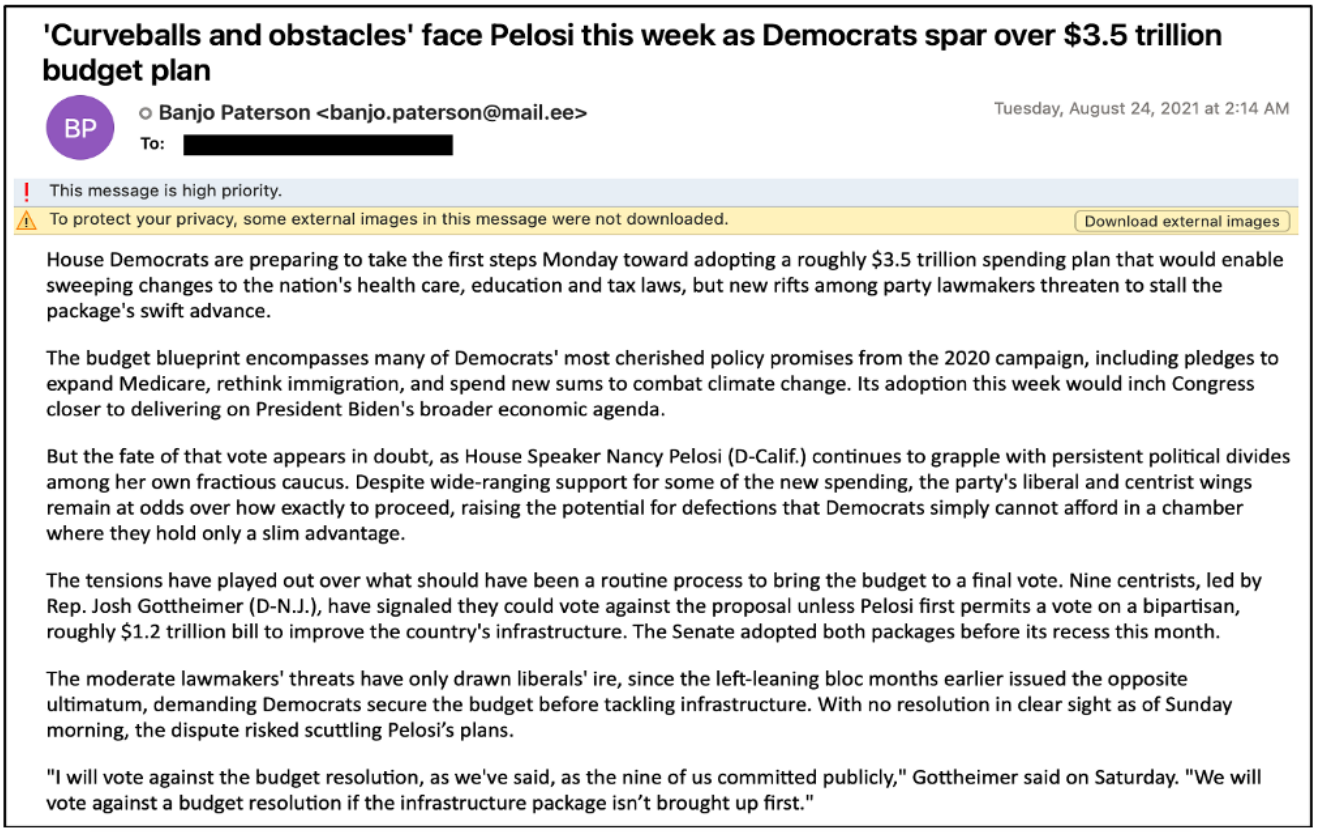
The campaigns by TA412 and their ilk evolved over the course of months, adjusting lures to best fit the current US political environment and switching to target US-based journalists focused on different areas of interest to the Chinese government. The campaigns which targeted journalists were part of a broader pattern of reconnaissance phishing conducted by this threat actor over many years.

2021: Between January and February 2021, Proofpoint researchers identified five campaigns by TA412 targeting US-based journalists, most notably those covering US politics and national security during events that gained international attention. Of note a very abrupt shift in targeting of reconnaissance phishing occurred in the days immediately preceding the 6 January 2021 attack on the US Capitol Building. Proofpoint researchers observed a focus on Washington DC and White House correspondents during this time. The malicious emails utilized subject lines pulled from recent US news articles, such as “Jobless Benefits Run Out as Trump Resists Signing Relief Bill,” “US issues Russia threat to China,” and “Trump Call to Georgia Official Might Violate State and Federal Law.”

The message bodies duplicated text included in the news articles and the web beacon URLs included a benign PNG file with a 0x0 aspect ratio that was retrieved as part of the web beacon in the following format:

> hxxp://www.actor-controlled domain[.]com/Free/<Targeted User Email Fragment>/0103/Customer.png.

The URL structure designates an actor-controlled domain, a campaign identifier, a victim identifier, a campaign date, and the name of the benign PNG resource.



'Curveballs and obstacles' face Pelosi this week as Democrats spar over $3.5 trillion budget plan

○ Banjo Paterson <banjo.paterson@mail.ee>

Tuesday, August 24, 2021 at 2:14 AM

To: [redacted]

! This message is high priority.

⚠ To protect your privacy, some external images in this message were not downloaded.

House Democrats are preparing to take the first steps Monday toward adopting a roughly $3.5 trillion spending plan that would enable sweeping changes to the nation's health care, education and tax laws, but new rifts among party lawmakers threaten to stall the package's swift advance.

The budget blueprint encompasses many of Democrats' most cherished policy promises from the 2020 campaign, including pledges to expand Medicare, rethink immigration, and spend new sums to combat climate change. Its adoption this week would inch Congress closer to delivering on President Biden's broader economic agenda.

But the fate of that vote appears in doubt, as House Speaker Nancy Pelosi (D-Calif.) continues to grapple with persistent political divides among her own fractious caucus. Despite wide-ranging support for some of the new spending, the party's liberal and centrist wings remain at odds over how exactly to proceed, raising the potential for defections that Democrats simply cannot afford in a chamber where they hold only a slim advantage.

The tensions have played out over what should have been a routine process to bring the budget to a final vote. Nine centrists, led by Rep. Josh Gottheimer (D-N.J.), have signaled they could vote against the proposal unless Pelosi first permits a vote on a bipartisan, roughly $1.2 trillion bill to improve the country's infrastructure. The Senate adopted both packages before its recess this month.

The moderate lawmakers' threats have only drawn liberals' ire, since the left-leaning bloc months earlier issued the opposite ultimatum, demanding Democrats secure the budget before tackling infrastructure. With no resolution in clear sight as of Sunday morning, the dispute risked scuttling Pelosi’s plans.

"I will vote against the budget resolution, as we've said, as the nine of us committed publicly," Gottheimer said on Saturday. "We will vote against a budget resolution if the infrastructure package isn’t brought up first."

Figure 1. Sample of a TA412 web beacon reconnaissance email. If an email client is configured to block downloadable content, then the web beacon URL should be presented to the target with an option to download the remote content, as seen in this image.

In August 2021, after a months-long break, TA412 again turned to targeting journalists, but this time those working cybersecurity, surveillance, and privacy issues with a focus on China. Those targeted appeared to have written extensively on social media privacy issues and Chinese disinformation campaigns, signaling an interest by the Chinese state in media narratives that could push a negative global opinion or perception of China. These campaigns mirrored those identified earlier in 2021 but demonstrated an evolving web beacon URL structure that changes over time. The observed structure was:

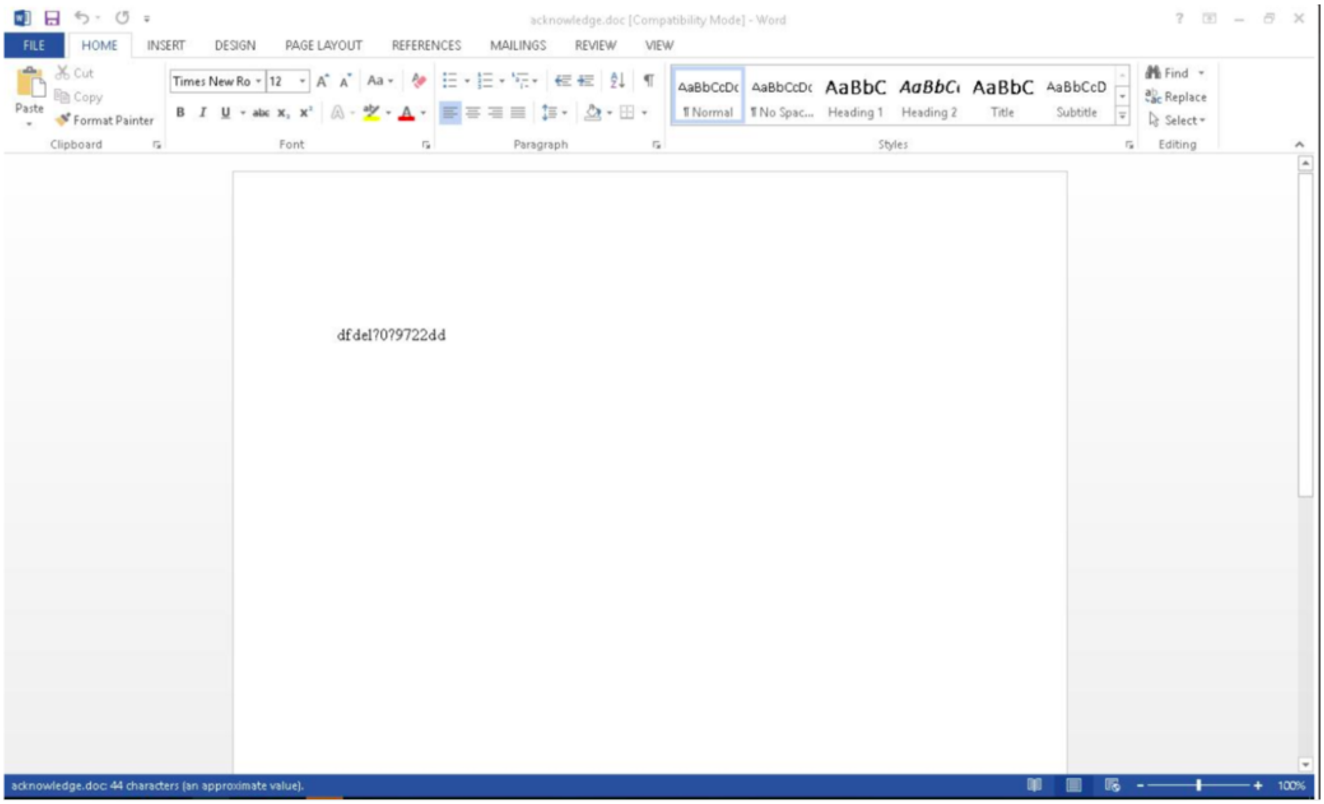
> hxxp://[actor-controlled domain/IP]/stringhere/AbbreviatedVictimAddress[@]AbbreviatedTargetedOrganization/filename[.]png.

2022: After an observed pause in targeting journalists, Proofpoint researchers identified a resumption of targeting this sector on February 9, 2022. The campaigns were numerous and occurred over a period of ten days. These campaigns strongly resembled those noted in early 2021 and indicated a desire to collect on US-based media organizations and contributors with a focus on those reporting on US and European engagement in the anticipated Russia-Ukraine war.

Subjects included:

- New bill aims to prohibit US military aid to Ukraine
- US issues Russia threat to China
- Macron reveals Putin 'guarantees'
- UK to arm Ukraine with anti-ship missiles against Russia - Kiev's envoy
- US says how Ukraine stand-off can be resolved
- UK says invasion 'highly likely'
- White House says door for diplomacy with Russia remains open, but troop buildup is continuing

Another Chinese APT group, **TA459**, in late April 2022 targeted media personnel with emails containing a malicious Royal Road RTF attachment (acknowledge.doc) that, if opened, would install and execute Chinoxy malware. This malware is a backdoor that is used to gain persistence on a victim's machine. Researchers at Bitdefender have observed the threat actor's use of Chinoxy extensively in Southeast Asia since at least 2018. Of note, the targeted entity was responsible for reporting on the Russia-Ukraine conflict, which aligns with TA459's historic mandate of collecting on intelligence matters related to Russia and Belarus.



dfdel7079722dd

acknowledge.doc: 44 characters (an approximate value).

Figure 2. The Word document attachment, file name acknowledge.doc.

This campaign used a possibly compromised Pakistani government email address to send the emails and looked to entice media recipients with a lure on foreign policy in Afghanistan. To add to the credibility of the emails, TA459 included links to a benign YouTube video produced by the Islamabad Security Dialogue, which references disinformation campaigns.

Session IV - Navigating Disinformation and Discourse in the Information Age | ISD 2022

12 views • Apr 27, 2022

Figure 3. Screenshot of the YouTube video link included in the malicious emails.

North Korea

In a vengeful twist, the North Korea-aligned **TA404** in early 2022 targeted a US-based media organization with job opportunity-themed phishing. This attack occurred after the organization published an article critical of North Korean leader Kim Jong Un—a well-known motivator for action by North Korea-aligned APT actors. TA404, known more broadly as Lazarus, typically engages in highly targeted campaigns that begin with benign messages. This campaign aligned with that expected behavior. It started with reconnaissance phishing that used URLs customized to each recipient. The URLs impersonated a job posting with landing pages designed to look like a branded job posting site. If a victim interacted with the URL, which contained a unique target ID, the server resolving the domain would have received confirmation that the email was delivered, and the intended target had interacted with it. This request also provides identifying information about the computer, or device, allowing the host to keep track of the intended target.

While Proofpoint researchers did not observe follow-up emails, considering this threat actor's proclivity for later sending malware-laden email attachments, it is likely that TA404 would have attempted to send malicious template document attachment or something similar in the future. Researchers at the Google Threat Analysis Group (TAG) on March 24, 2022 disclosed details on this campaign as part of "Operation Dream Job." While journalism and media were not listed among the targeted sectors, Proofpoint has observed shared indicators of compromise utilized in both campaigns identified earlier this year and those reported by Google TAG.

Targeting Journalists’ Social Media Accounts

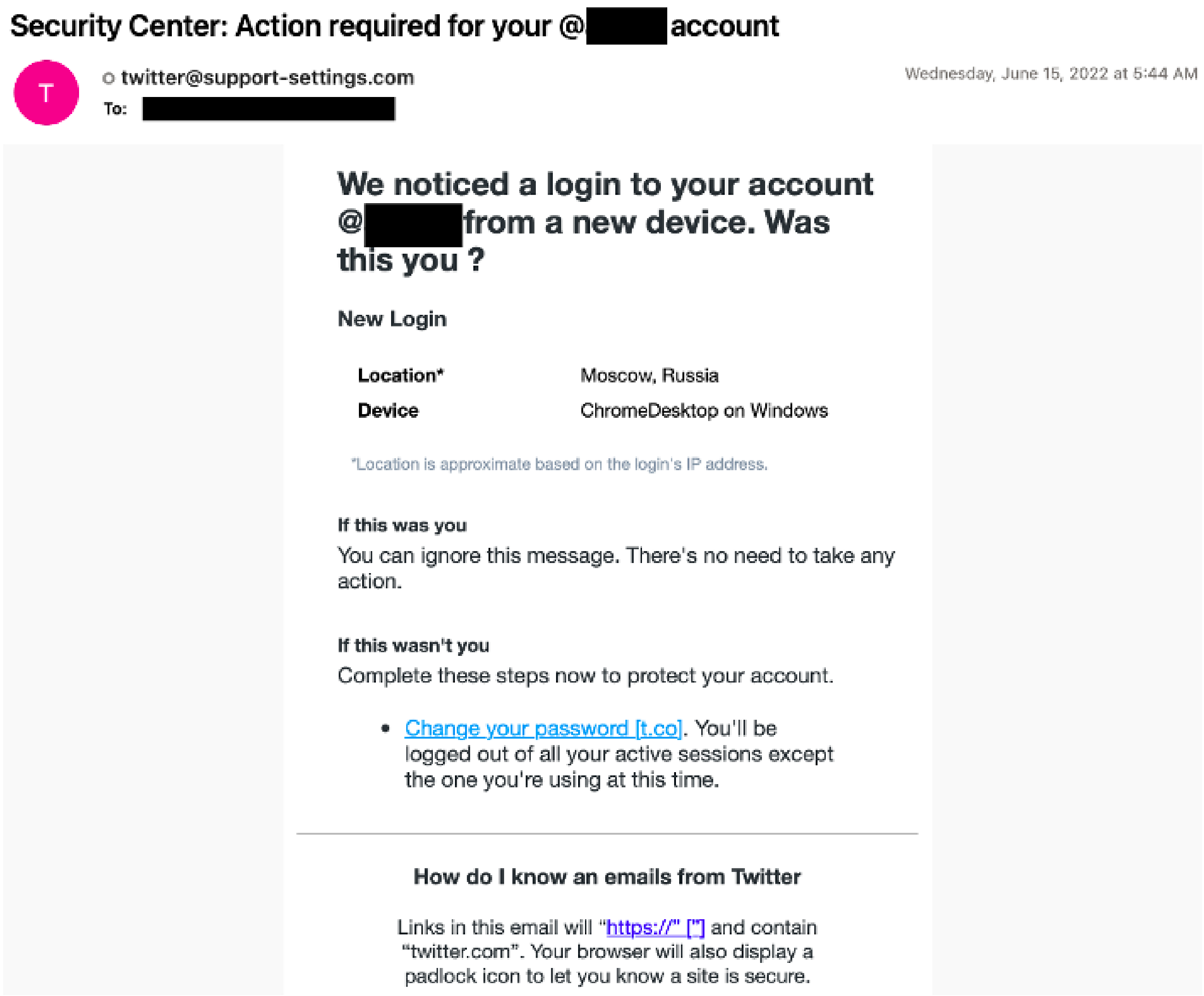
Targeting journalists and media organizations for their social media account credentials can have significant consequences. For example, in 2013 a threat actor took over the official Associated Press Twitter account and posted a tweet claiming President Barack Obama had been injured in an attack on the White House. The stock market dropped more than 100 points in roughly two minutes following the tweet. Two years later, in 2015, a threat actor compromised about 130 Twitter accounts of influential individuals and tricked some of their followers into transferring more than $100,000 in Bitcoin to attacker-controlled accounts.

While often times campaigns looking to compromise social media accounts, including those by APTs, do not result in such severe or observable outcomes, they can still wind up requiring more than just an account reset or the activation of multi-factor authentication (MFA), especially since enabling MFA is not a guarantee of complete account protection.

Turkey

Since early 2022, Proofpoint researchers have observed a prolific threat actor, tracked as **TA482**, regularly engaging in credential harvesting campaigns that target the social media accounts of mostly US-based journalists and media organizations. This victimology, TA482’s use of services originating from Turkey to host its domains and infrastructure, as well as Turkey’s history of leveraging social media to spread pro-President Recep Tayyip Erdogan and pro-Justice and Development Party (Turkey’s ruling party) propaganda support Proofpoint’s assessment that TA482 is aligned with the Turkish state.

Ongoing campaigns have narrowed in on Twitter credentials of any individuals that write for media publications. This includes journalists from well-known news outlets to those writing for an academic institution and everything in-between. The malicious emails are typically Twitter security themed and attempt to grab a recipient’s attention with subjects alerting the user to a suspicious or new login location.



Security Center: Action required for your @[redacted] account

twitter@support-settings.com

To: [redacted]

Wednesday, June 15, 2022 at 5:44 AM

We noticed a login to your account @[redacted] from a new device. Was this you ?

New Login

Location*	Moscow, Russia
Device	ChromeDesktop on Windows

*Location is approximate based on the login's IP address.

If this was you

You can ignore this message. There's no need to take any action.

If this wasn't you

Complete these steps now to protect your account.

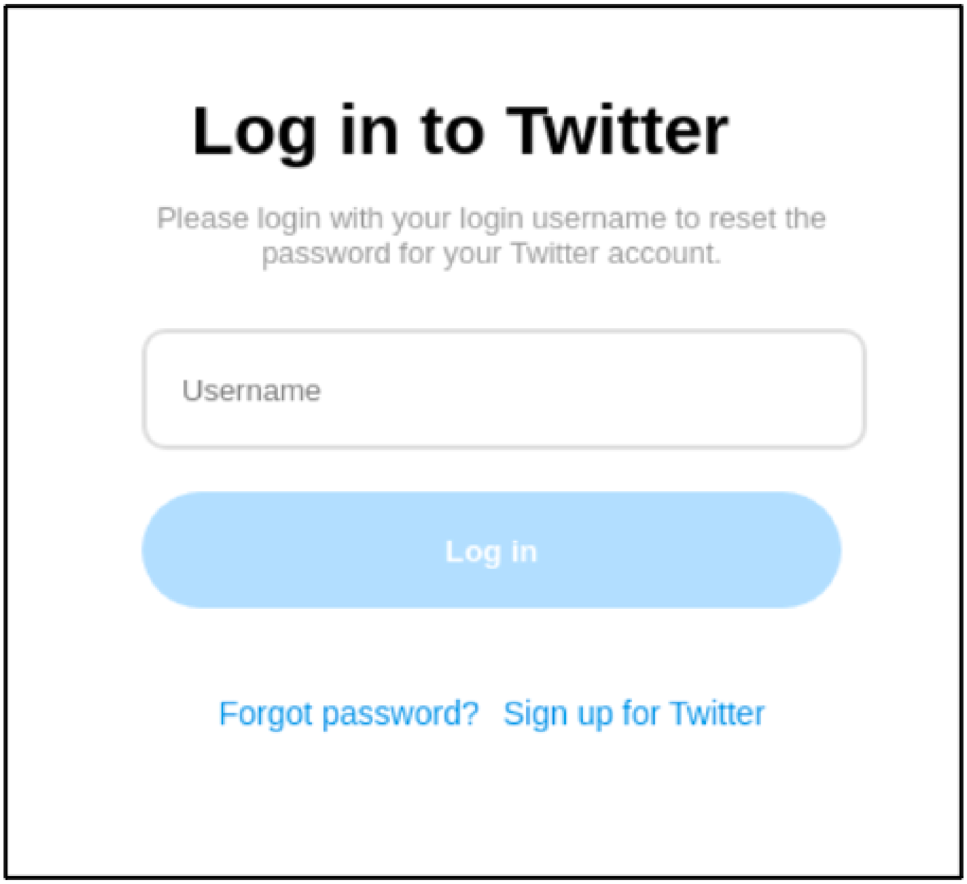
- Change your password [t.co]. You'll be logged out of all your active sessions except the one you're using at this time.

How do I know an emails from Twitter

Links in this email will "https://" ["] and contain "twitter.com". Your browser will also display a padlock icon to let you know a site is secure.

Figure 4. A typical TA482 Twitter-themed credential phishing email.

If the target clicks on the link supplied in the email, they are taken to a credential harvesting landing page which impersonates a Twitter login page to reset their password.



Log in to Twitter

Please login with your login username to reset the password for your Twitter account.

Figure 5. A TA482 landing page designed to steal a user’s credentials.

Proofpoint researchers cannot independently verify the motivations behind these campaigns, but the possibilities abound and, based on historical Turkey threat actor activity, could include using the compromised accounts to target a journalist’s social media contacts, use the accounts for defacement, or to spread propaganda. It is possible these attacks will ramp up as Turkey’s 2023 parliamentary and presidential elections draw near.

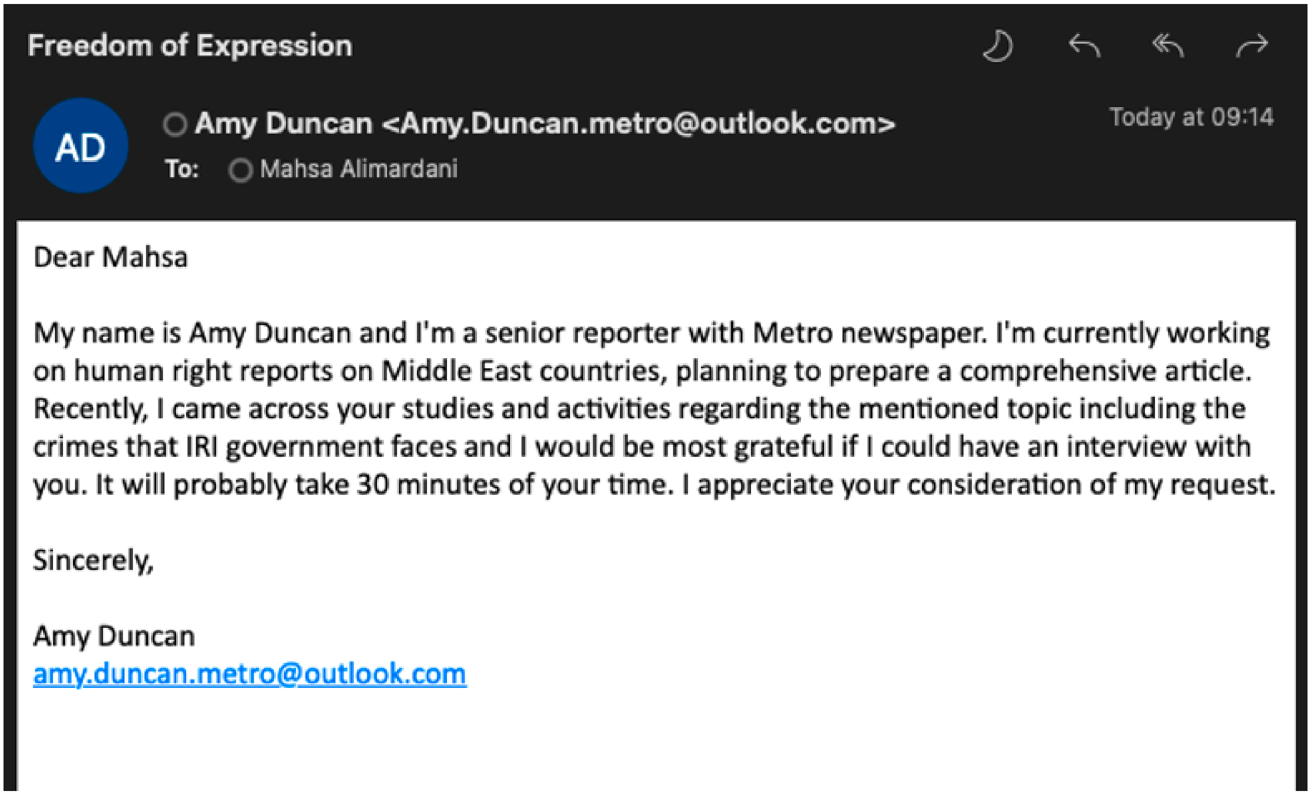
Posing as Journalists

There is an inherent sense of intrigue when one is approached by a journalist to discuss an area of expertise. The allure of having research highlighted in the media is often a great motivator to overlook or disregard signs that this opportunity may not be entirely legitimate. This social engineering tactic successfully exploits the human desire for recognition and is being leveraged by APT actors wishing to target academics and foreign policy experts worldwide, likely in an effort to gain access to sensitive information.

Iran

Multiple Iran-aligned APT actors use journalists or newspapers as pretexts to surveil targets and attempt to harvest their credentials. One of the most active in Proofpoint telemetry is **TA453**, also known as Charming Kitten. TA453, which we assess with high confidence supports the Islamic Revolutionary Guard Corps intelligence collection efforts, routinely masquerades as journalists from around the world. The threat actor uses these personas to engage in benign conversations with targets, which consist mostly of academics and policy experts working on Middle Eastern foreign affairs.

As can be seen in Figure 6, the content of TA453's initial outreach emails indicate a degree of research on the intended target likely to enhance the believability of the request and to encourage further dialogue.



Freedom of Expression

AD ○ Amy Duncan <Amy.Duncan.metro@outlook.com>
To: ○ Mahsa Alimardani

Today at 09:14

Dear Mahsa

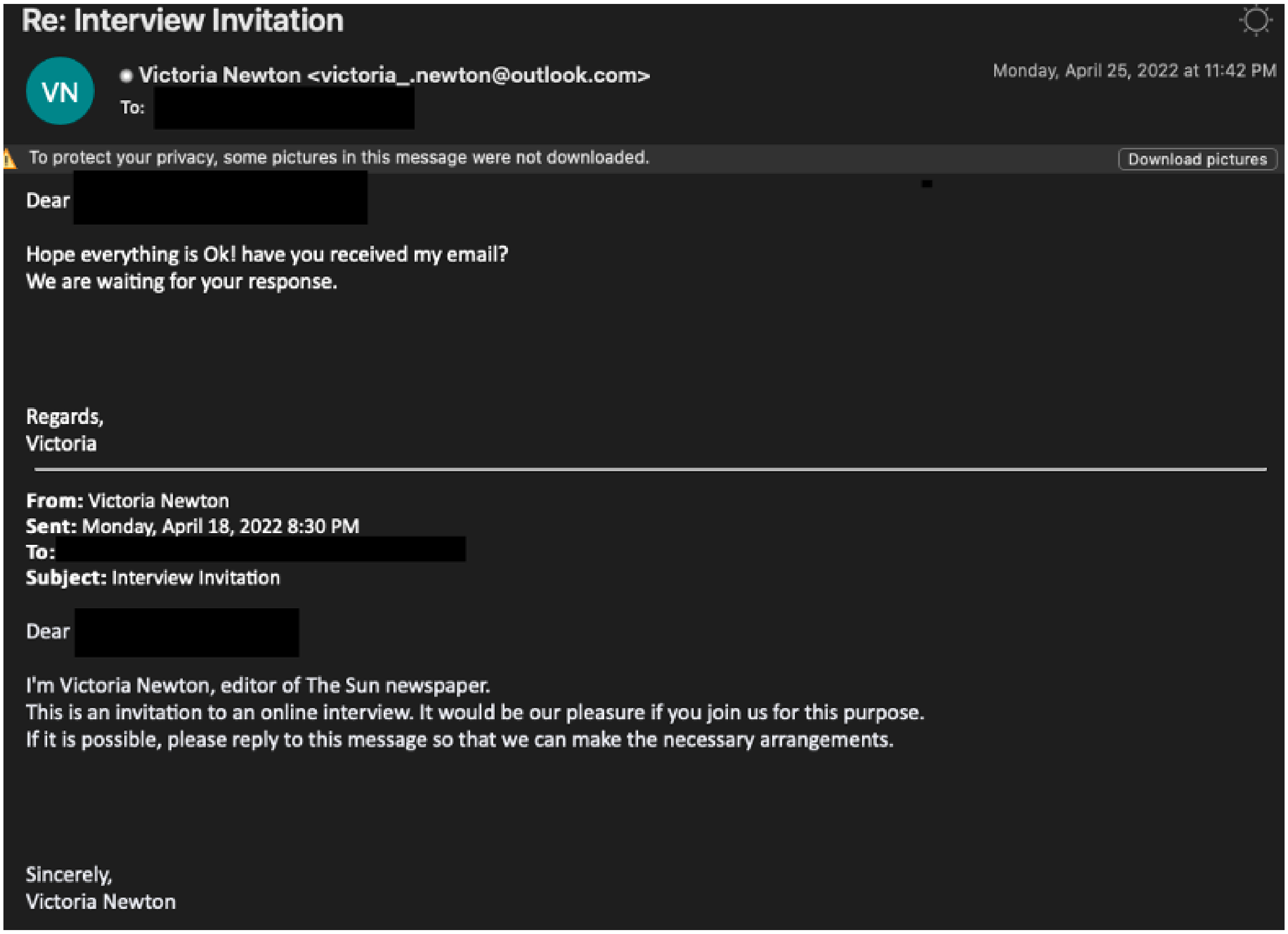
My name is Amy Duncan and I'm a senior reporter with Metro newspaper. I'm currently working on human right reports on Middle East countries, planning to prepare a comprehensive article. Recently, I came across your studies and activities regarding the mentioned topic including the crimes that IRI government faces and I would be most grateful if I could have an interview with you. It will probably take 30 minutes of your time. I appreciate your consideration of my request.

Sincerely,

Amy Duncan
amy.duncan.metro@outlook.com

Figure 6. Screenshot of a benign TA453 conversation starter, posted by and used with permission from Mahsa Alimardani via Twitter.

If the initial email is ignored, TA453 will often recontact individuals to follow up (Figure 7). If the targeted recipient does engage in conversation with the persona, TA453 will eventually invite them to a virtual meeting to have further discussions via a customized, but benign PDF (Figure 8).



Re: Interview Invitation

Victoria Newton <victoria_.newton@outlook.com>

To: [redacted]

Monday, April 25, 2022 at 11:42 PM

To protect your privacy, some pictures in this message were not downloaded.

Dear [redacted]

Hope everything is Ok! have you received my email?
We are waiting for your response.

Regards,
Victoria

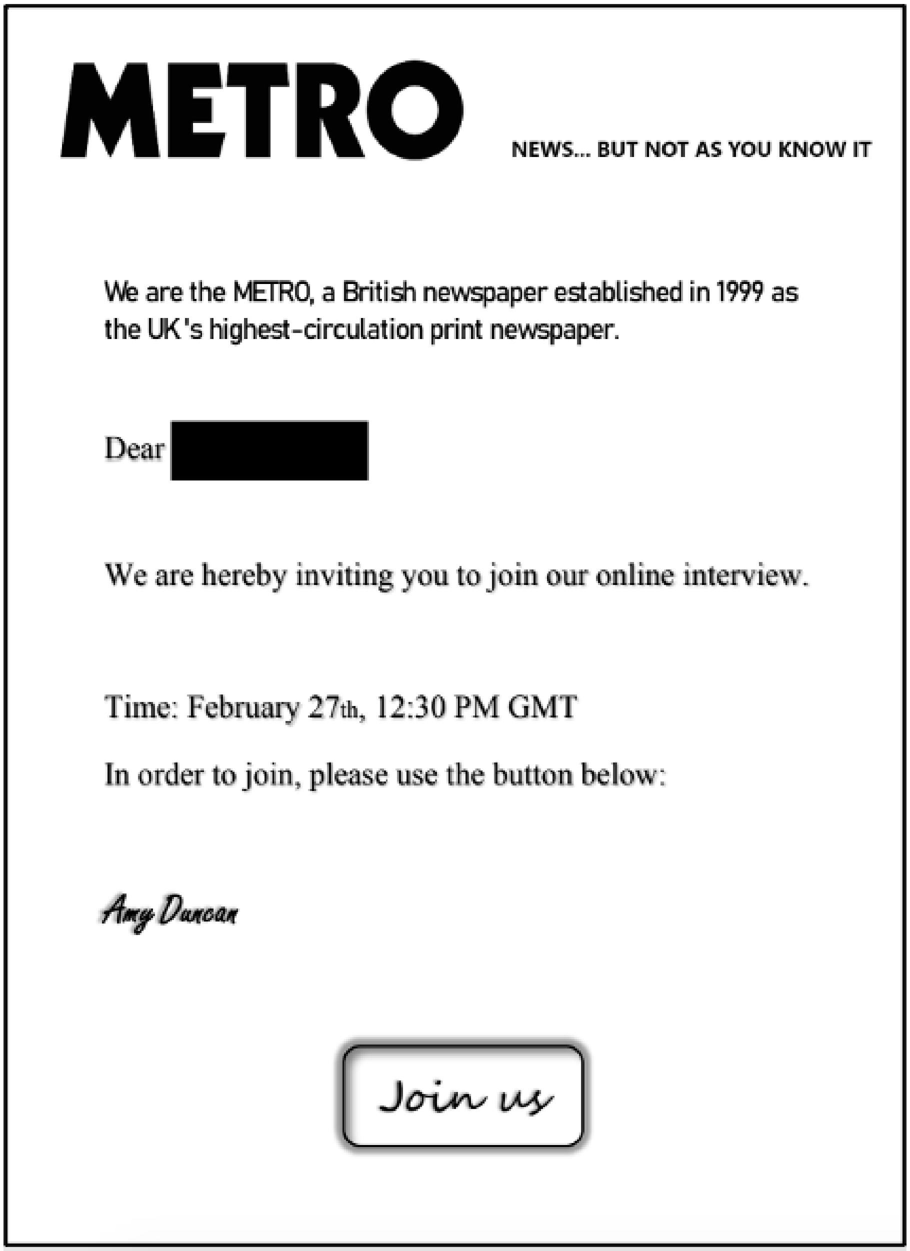
From: Victoria Newton
Sent: Monday, April 18, 2022 8:30 PM
To: [redacted]
Subject: Interview Invitation

Dear [redacted]

I'm Victoria Newton, editor of The Sun newspaper.
This is an invitation to an online interview. It would be our pleasure if you join us for this purpose.
If it is possible, please reply to this message so that we can make the necessary arrangements.

Sincerely,
Victoria Newton

Figure 7. Example of a TA453 follow-up email attempting to solicit a response from the target.



METRO NEWS... BUT NOT AS YOU KNOW IT

We are the METRO, a British newspaper established in 1999 as the UK's highest-circulation print newspaper.

Dear [redacted]

We are hereby inviting you to join our online interview.

Time: February 27th, 12:30 PM GMT

In order to join, please use the button below:

Amy Duncan

Join us

Figure 8. Example of a TA453 benign PDF uploaded to VirusTotal.

The vast majority of TA453 campaigns ultimately lead to credential harvesting. The benign PDFs, similar to Figure 8, are typically delivered from file hosting services and almost always contain a link to a URL shortener and IP tracker that redirects targets to the credential harvesting domains on actor-controlled infrastructure.

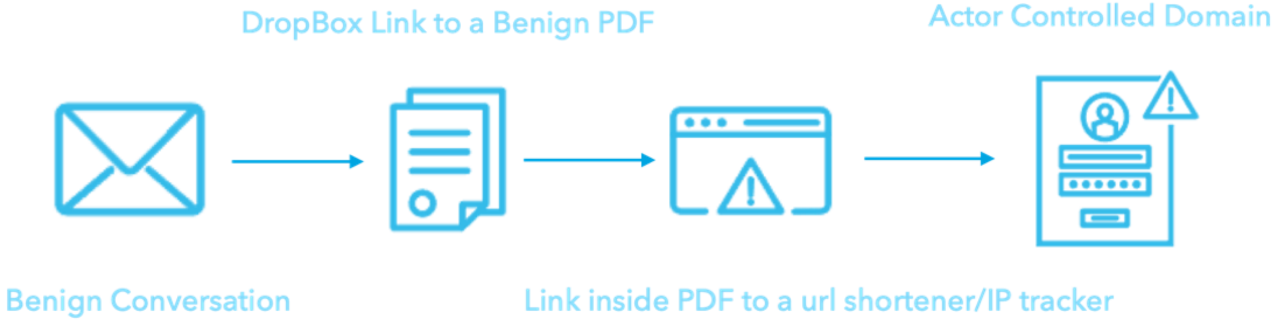
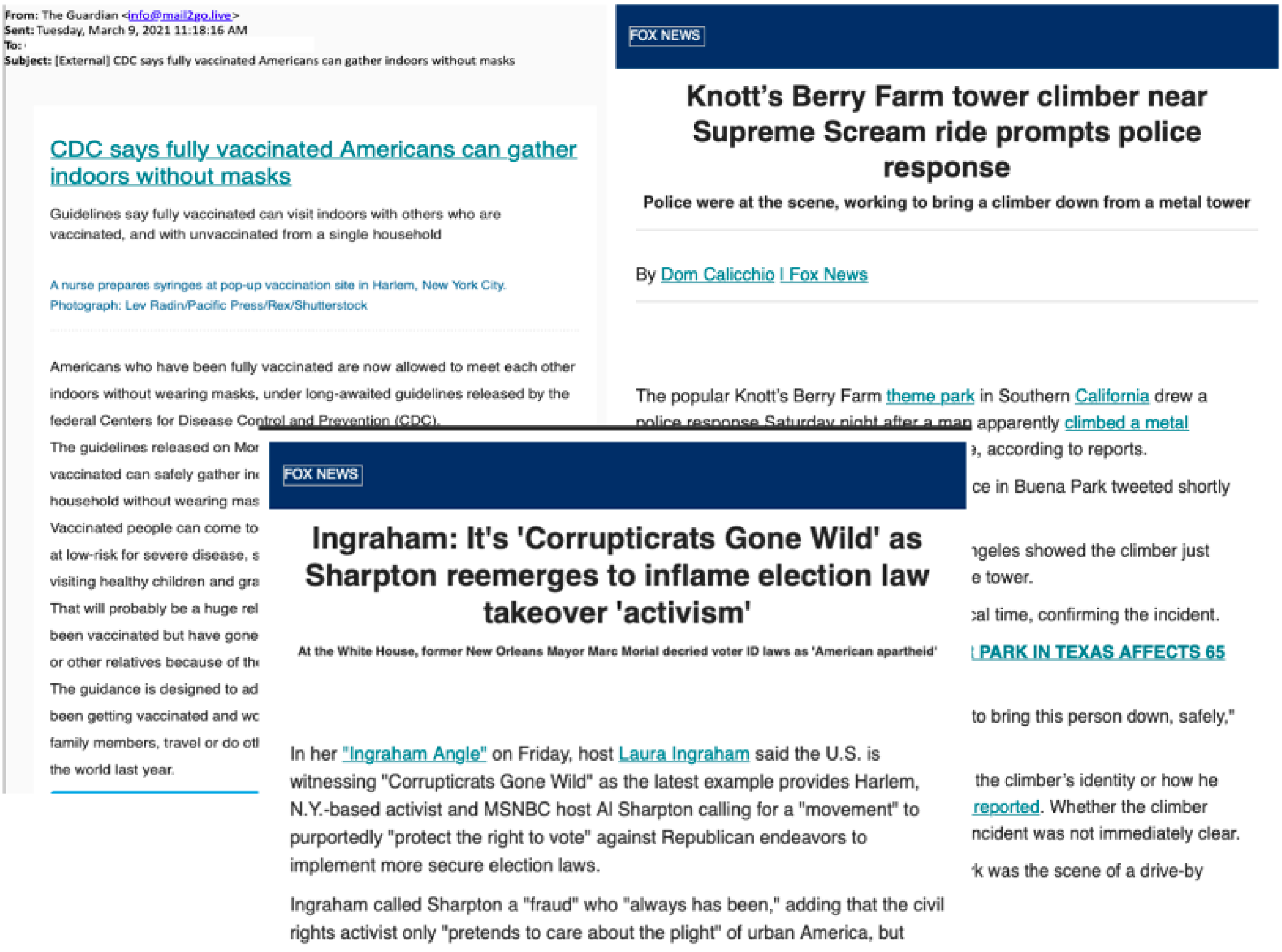

DropBox Link to a Benign PDF
Actor Controlled Domain
Benign Conversation
Link inside PDF to a url shortener/IP tracker

Figure 9. Standard TA453 attack chain.

TA456, also known as Tortoiseshell, is another Iran-aligned threat actor that routinely masquerades as media organizations sending newsletters across the ideological spectrum, including Fox News and the Guardian. TA456 has repeatedly targeted the same users with newsletter themed emails containing web beacons. This activity likely has complemented TA456's efforts to deliver malware via relationships built on social media similar to previous campaigns.



From: The Guardian <info@mail2go.live>
Sent: Tuesday, March 9, 2021 11:18:16 AM
To:
Subject: [External] CDC says fully vaccinated Americans can gather indoors without masks

CDC says fully vaccinated Americans can gather indoors without masks

Guidelines say fully vaccinated can visit indoors with others who are vaccinated, and with unvaccinated from a single household

A nurse prepares syringes at pop-up vaccination site in Harlem, New York City. Photograph: Lev Radin/Pacific Press/Rex/Shutterstock

Americans who have been fully vaccinated are now allowed to meet each other indoors without wearing masks, under long-awaited guidelines released by the federal Centers for Disease Control and Prevention (CDC).

The guidelines released on Mor
vaccinated can safely gather in
household without wearing mas
Vaccinated people can come to
at low-risk for severe disease, s
visiting healthy children and gra
That will probably be a huge rel
been vaccinated but have gone
or other relatives because of th
The guidance is designed to ad
been getting vaccinated and wc
family members, travel or do otl
the world last year.

FOX NEWS

Knott's Berry Farm tower climber near Supreme Scream ride prompts police response

Police were at the scene, working to bring a climber down from a metal tower

By Dom Calicchio | Fox News

The popular Knott's Berry Farm theme park in Southern California drew a police response Saturday night after a man apparently climbed a metal
e, according to reports.
ce in Buena Park tweeted shortly

ngeles showed the climber just
e tower.

cal time, confirming the incident.

PARK IN TEXAS AFFECTS 65

to bring this person down, safely,"

the climber's identity or how he
reported. Whether the climber
ncident was not immediately clear.

k was the scene of a drive-by

FOX NEWS

Ingraham: It's 'Corrupticrats Gone Wild' as Sharpton reemerges to inflame election law takeover 'activism'

At the White House, former New Orleans Mayor Marc Morial decried voter ID laws as 'American apartheid'

In her "Ingraham Angle" on Friday, host Laura Ingraham said the U.S. is witnessing "Corrupticrats Gone Wild" as the latest example provides Harlem, N.Y.-based activist and MSNBC host Al Sharpton calling for a "movement" to purportedly "protect the right to vote" against Republican endeavors to implement more secure election laws.

Ingraham called Sharpton a "fraud" who "always has been," adding that the civil rights activist only "pretends to care about the plight" of urban America, but

Figure 10. Examples of the newsletter-themes used by TA456 in the bodies of their phishing emails.

Lastly, **TA457**, an Iran-aligned threat actor active in Proofpoint data since late 2021, has been known to masquerade as an “iNews Reporter” to deliver malware to public relations personnel for companies located in the US, Israel, and Saudi Arabia. For example, in early March 2022, TA457 sent an email with the ironic subject “Iran Cyber War” and the actor-controlled domain news-spot[.]live. The campaign continued TA457’s pattern of using news themed lure websites to deliver a malicious URL. The URL structure (news-spot[.]live/Reports/1/?id=[Campaign/Lure Identifier]&pid=[TargetIdentifier]) has both an identifier to track which lure documents to deliver along with a PID to determine which recipient is receiving the phish. The themes of documents have included Iran, Russia, drones, war crimes, “secret weapons,” and more. When a user clicks the malicious URL, two files are downloaded: a Word document and an .scr file. When macros are enabled on the document, it drops an embedded executable file (DnsDig.exe). When the reader.scr file is dropped, it downloads DnsDig.exe from the URL and also drops iran.pdf as a decoy to the user. DnsDig is a TA457 remote access trojan that uses DNS tunneling to a hardcoded domain (cyberclub[.]one). *Figure 11. Attack chain of TA457 “Iran Cyber War” campaign.*

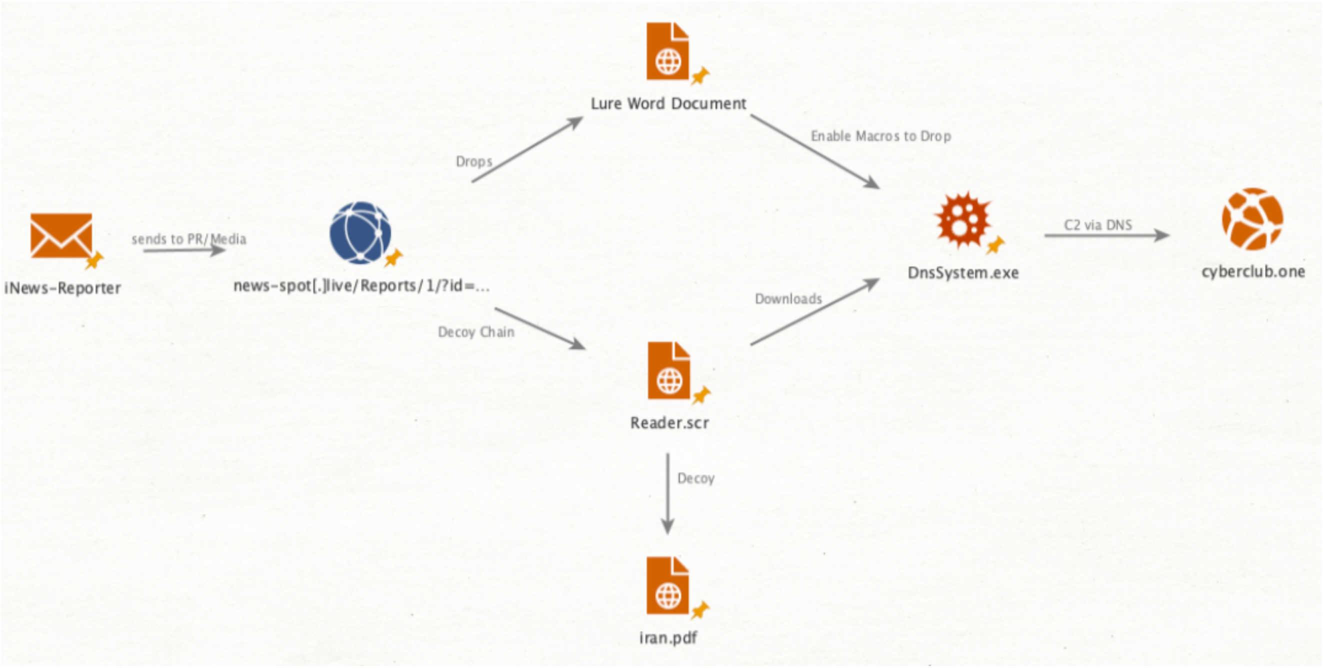


Figure 11. Attack chain of TA457 “Iran Cyber War” campaign.

Between September 2021 and March 2022, Proofpoint observed TA457 campaigns approximately every two to three weeks. The March 2022 campaign targeted both individual and generic, group email addresses such as international.media@[redacted].com at less than ten Proofpoint customers involved in energy, media, government, and manufacturing.

Conclusion

Targeting journalists and media organizations is not novel. APT actors, regardless of their state affiliation, have and will likely always have a mandate to target journalists and media organizations and will use associated personas to further their objectives and collection priorities. From intentions to gather sensitive information to attempts to manipulate public perceptions, the knowledge and access that a journalist or news outlet can provide is unique in the public space. Targeting the media sector also lowers the risk of failure or discovery to an APT actor than going after other, more hardened targets of interest, such as government entities.

The varied approaches by APT actors—using web beacons for reconnaissance, credential harvesting, and sending malware to gain a foothold in a recipient's network—means those operating in the media space need to stay vigilant. Assessing one's personal level of risk can give an individual a good sense of the odds they will end up as a target. Such as, if you report on China or North Korea or associated threat actors, you may become part of their collection requirements in the future. Being aware of the broad attack surface—all the varied online platforms used for sharing information and news—an APT actor can leverage is also key to preventing oneself from becoming a victim. And ultimately practicing caution and verifying the identity or source of an email can halt an APT attack in its nascent stage.

Previous Blog Post
Subscribe to the Proofpoint Blog