How we're tackling evolving online threats

blog.google/threat-analysis-group/how-were-tackling-evolving-online-threats

Shane Huntley

October 16, 2020

Threat Analysis Group

Major events like elections and COVID-19 present opportunities for threat actors, and Google's Threat Analysis Group (TAG) is working to thwart these threats and protect our products and the people using them. As we head into the U.S. election, we wanted to share

an update on what we're seeing and how threat actors are changing their tactics.

What we're seeing around the U.S. elections

In June, we announced that we saw phishing attempts against the personal email accounts of staffers on the Biden and Trump campaigns by Chinese and Iranian APTs (Advanced Persistent Threats) respectively. We haven't seen any evidence of such attempts being successful.

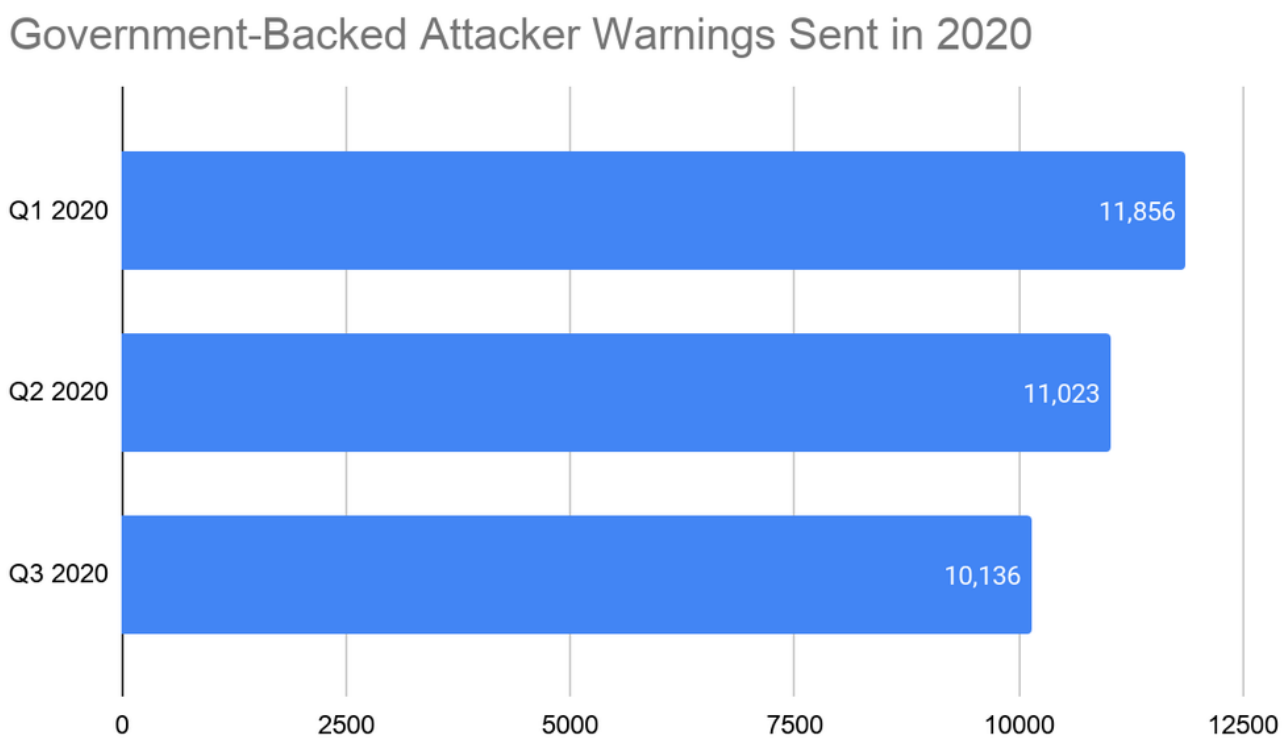
The Iranian attacker group (APT35) and the Chinese attacker group (APT31) targeted campaign staffers' personal emails with credential phishing emails and emails containing tracking links. As part of our wider tracking of APT31 activity, we've also seen them deploy targeted malware campaigns.

One APT31 campaign was based on emailing links that would ultimately download malware hosted on GitHub. The malware was a python-based implant using Dropbox for command and control. It would allow the attacker to upload and download files as well as execute arbitrary commands. Every malicious piece of this attack was hosted on legitimate services, making it harder for defenders to rely on network signals for detection.

In one example, attackers impersonated McAfee. The targets would be prompted to install a legitimate version of McAfee anti-virus software from GitHub, while malware was simultaneously silently installed to the system.

Example prompt from an APT31 campaign impersonating McAfee

When we detect that a user is the target of a government-backed attack, we send them a prominent warning. In these cases, we also shared our findings with the campaigns and the Federal Bureau of Investigation. This targeting is consistent with what others have subsequently reported.



Number of “government backed attacker” warnings sent in 2020

Overall, we’ve seen increased attention on the threats posed by APTs in the context of the U.S. election. U.S government agencies have warned about different threat actors, and we’ve worked closely with those agencies and others in the tech industry to share leads and intelligence about what we’re seeing across the ecosystem. This has resulted in action on our platforms, as well as others. Shortly after the U.S. Treasury sanctioned Ukrainian Parliament member Andrii Derkach for attempting to influence the U.S. electoral process, we removed 14 Google accounts that were linked to him.

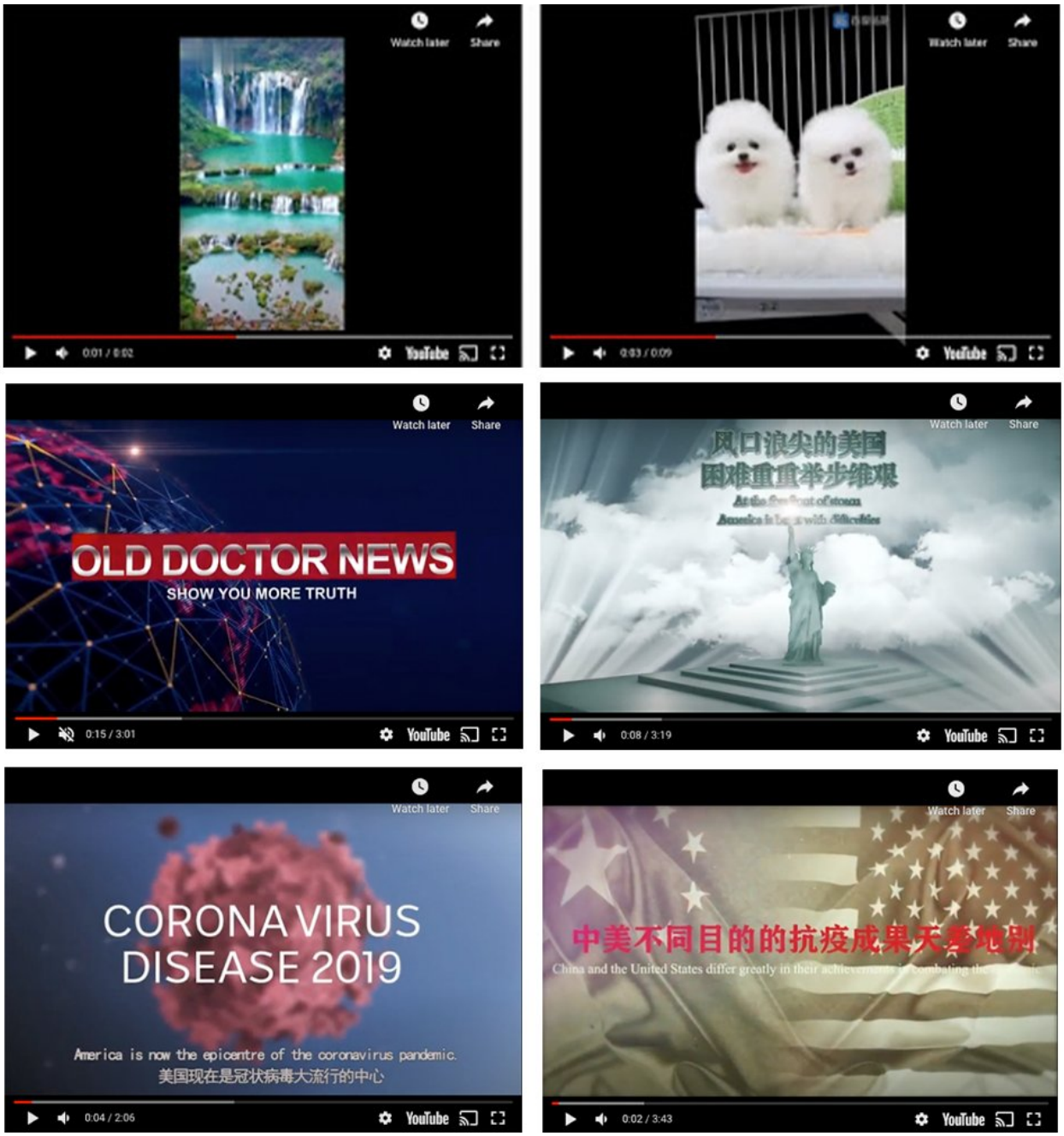
Coordinated influence operations

We’ve been sharing actions against coordinated influence operations in our quarterly TAG bulletin (check out our Q1, Q2 and Q3 updates). To date, TAG has not identified any significant coordinated influence campaigns targeting, or attempting to influence, U.S. voters on our platforms.

Since last summer, TAG has tracked a large spam network linked to China attempting to run an influence operation, primarily on YouTube. This network has a presence across multiple platforms, and acts by primarily acquiring or hijacking existing accounts and posting spammy content in Mandarin such as videos of animals, music, food, plants, sports, and games. A small fraction of these spam channels will then post videos about current events. Such videos frequently feature clumsy translations and computer-generated voices. Researchers at Graphika and FireEye have detailed how this network behaves—including its shift from

posting content in Mandarin about issues related to Hong Kong and China's response to COVID-19, to including a small subset of content in English and Mandarin about current events in the U.S. (such as protests around racial justice, the wildfires on the West Coast, and the U.S. response to COVID-19).

We've taken an aggressive approach to identifying and removing content from this network—for example, in Q3 alone, our Trust and Safety teams terminated more than 3,000 YouTube channels. As a result, this network hasn't been able to build an audience. Most of the videos we identify have fewer than 10 views, and most of these views appear to come from related spam accounts rather than actual users. So while this network has posted frequently, the majority of this content is spam and we haven't seen it effectively reach an actual audience on YouTube. We've shared our findings on this network in our Q2 and Q3 TAG bulletins and will continue to update there.

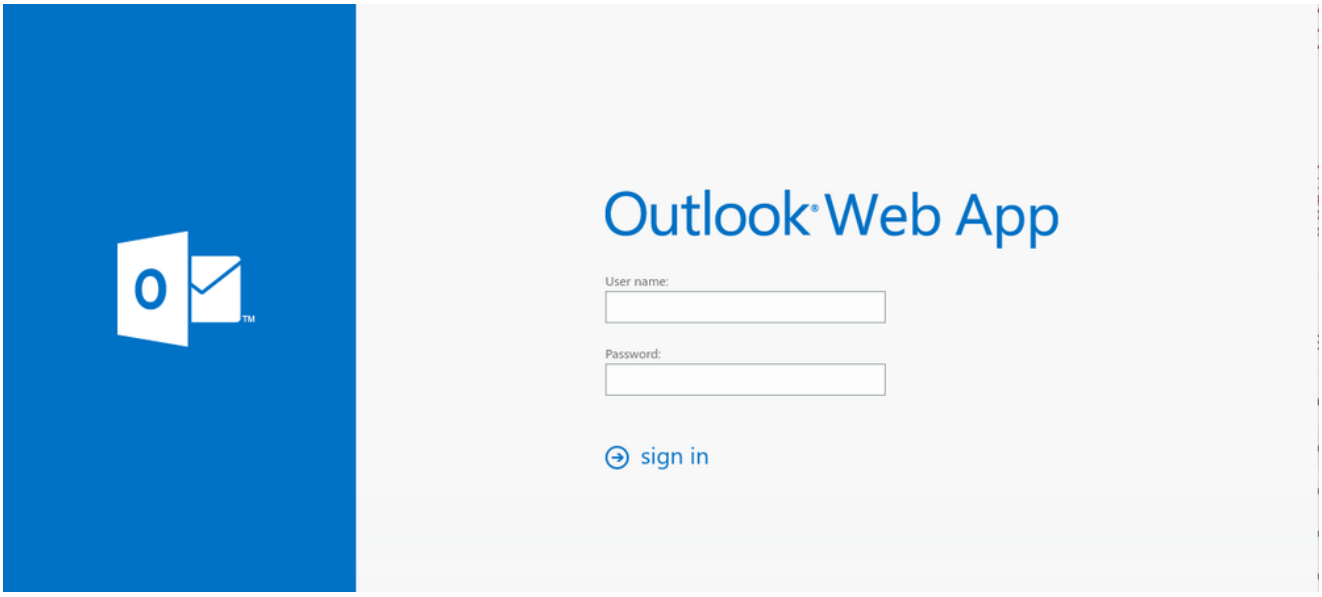


Examples of YouTube videos removed

New COVID-19 targets

As the course of the COVID-19 pandemic evolves, we've seen threat actors evolve their tactics as well. In previous posts, we discussed targeting of health organizations as well as attacker efforts to impersonate the World Health Organization. This summer, we and others observed threat actors from China, Russia and Iran targeting pharmaceutical companies and researchers involved in vaccine development efforts.

In September, we started to see multiple North Korea groups shifting their targeting towards COVID-19 researchers and pharmaceutical companies, including those based in South Korea. One campaign used URL shorteners and impersonated the target's webmail portal in an attempt to harvest email credentials. In a separate campaign, attackers posed as recruiting professionals to lure targets into downloading malware.



Spoofed Outlook login panel used by North Korean attackers attempting to harvest credentials

Tackling DDoS attacks as an industry

In the threat actor toolkit, different types of attacks are used for different purposes: Phishing campaigns can be used like a scalpel—targeting specific groups or individuals with personalized lures that are more likely to trick them into taking action (like clicking on a malware link), while DDoS attacks are more like a hatchet—disrupting or blocking a site or a service entirely. While it's less common to see DDoS attacks rather than phishing or hacking campaigns coming from government-backed threat groups, we've seen bigger players increase their capabilities in launching large-scale attacks in recent years. For example in 2017, our Security Reliability Engineering team measured a record-breaking UDP amplification attack sourced out of several Chinese ISPs (ASNs 4134, 4837, 58453, and 9394), which remains the largest bandwidth attack of which we are aware.

Addressing state-sponsored DDoS attacks requires a coordinated response from the internet community, and we work with others to identify and dismantle infrastructure used to conduct attacks. Going forward, we'll also use this blog to report attribution and activity we see in this space from state-backed actors when we can do so with a high degree of confidence and in a way that doesn't disclose information to malicious actors.

POSTED IN:

Threat Analysis Group