How we're protecting users from government-backed attacks from North Korea

Adam Weidemann ⋮⋮ 4/5/2023

New Threat Analysis Group reporting underscores the evolution of ARCHIPELAGO - as well as Google's work to stop government-backed attackers

As part of Threat Analysis Group (TAG)'s mission to counter serious threats to Google and our users, TAG has been tracking government-backed hacking activity tied to North Korea for over a decade. Today, as a follow up to Mandiant's report on APT43, we are sharing TAG's observations on this actor and what Google is doing to protect users from this group and other government-backed attackers. Because TAG's visibility into this actor is distinct from Mandiant's, TAG uses the name ARCHIPELAGO to track a subset of APT43 activity.

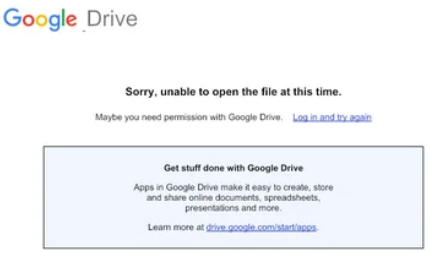
TAG began tracking ARCHIPELAGO in 2012 and has observed the group target individuals with expertise in North Korea policy issues such as sanctions, human rights and non-proliferation issues. These targets include Google and non-Google accounts belonging to government and military personnel, think tanks, policy makers, academics, and researchers in South Korea, the US and elsewhere.

To safeguard users at-risk, TAG uses our research on serious threat actors like ARCHIPELAGO to improve the safety and security of Google's products. TAG adds newly discovered malicious websites and domains to Safe Browsing to protect users from further exploitation. We also send all targeted Gmail and Workspace users government-backed attacker alerts notifying them of the activity. We encourage potential targets to enroll in Google's Advanced Protection Program, enable Enhanced Safe Browsing for Chrome and ensure that all devices are updated.

ARCHIPELAGO phishing: persistent and targeted

ARCHIPELAGO often sends phishing emails where they pose as a representative of a media outlet or think tank and ask North Korea experts to participate in a media interview or request for information (RFI). The emails prompt recipients to click a link to view the interview questions or RFI. When the recipient clicks, the link redirects to a phishing site that masquerades as a login prompt. The phishing page records keystrokes entered into the login form and sends them to an attacker-controlled URL. After the recipient enters their password, the phishing page redirects

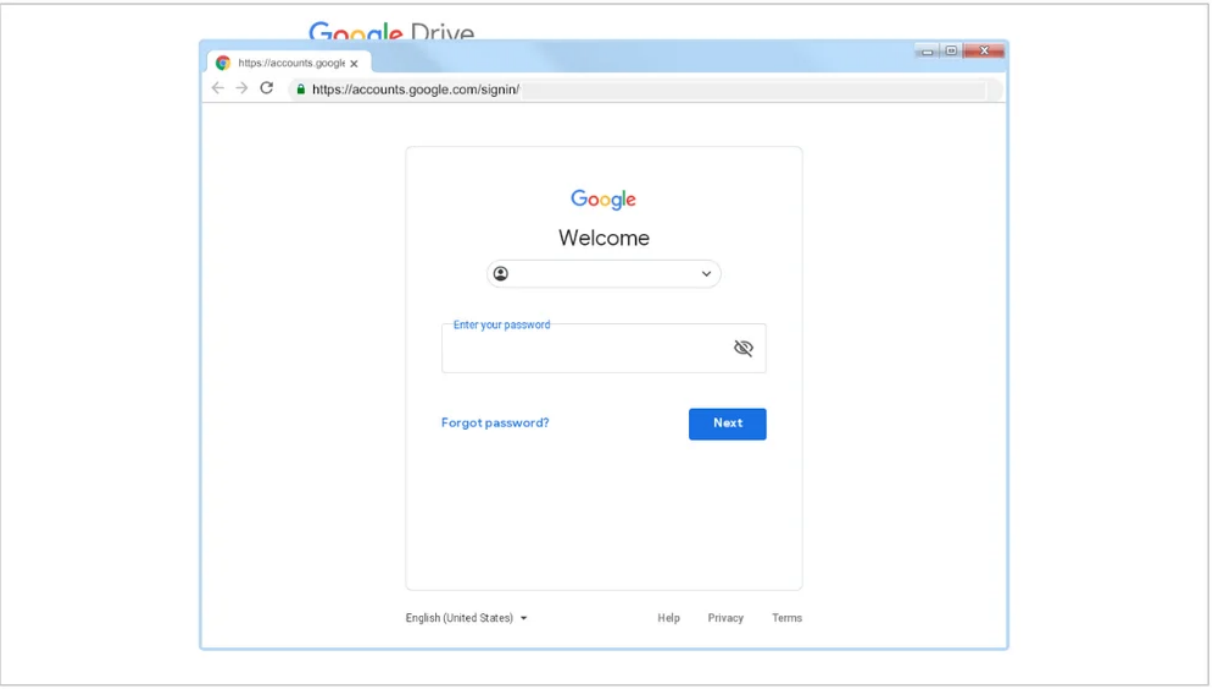
to a benign document with contextually appropriate interview questions, or an RFI that would make sense to the recipient based on the content of the original phishing email.



- Drive-themed phishing landing page ARCHIPELAGO used in combination with “interview request” phishing ema
-
-
-

ARCHIPELAGO invests time and effort to build rapport with targets, often corresponding with them by email over several days or weeks before finally sending a malicious link or file. In one case, the group posed as a journalist for a South Korean news agency and sent benign emails with an interview request to North Korea experts. When recipients replied expressing interest in an interview, ARCHIPELAGO continued the correspondence over several emails before finally sending a OneDrive link to a password-protected file that contained malware.

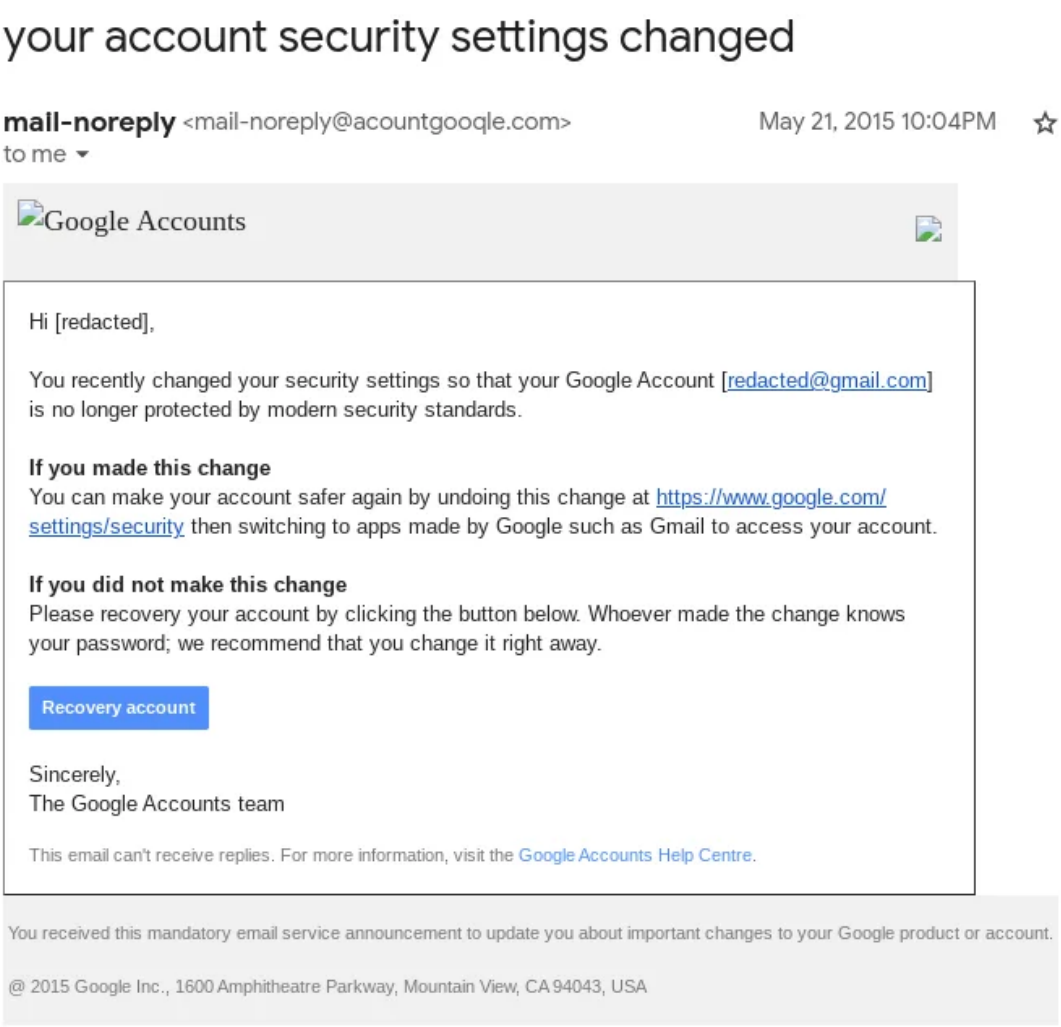
ARCHIPELAGO has also sent links that lead to “browser-in-the-browser” phishing pages. The phishing pages present users with a fake browser window rendered inside the actual browser window. The fake browser window displays a URL and a login prompt designed to trick users into thinking they are entering their password into a legitimate login page.



ARCHIPELAGO “browser-in-the-browser” phishing page

Shifting phishing tactics

ARCHIPELAGO has shifted their phishing tactics over time. For several years, they sent typical phishing messages that posed as Google Account security alerts. Over time this technique became less successful and ARCHIPELAGO has evolved and experimented with new phishing that might be more difficult for users and common security controls to catch.


your account security settings changed

mail-noreply <mail-noreply@acountgooqle.com> May 21, 2015 10:04PM

to me

Google Accounts

Hi [redacted],

You recently changed your security settings so that your Google Account [redacted@gmail.com] is no longer protected by modern security standards.

If you made this change
You can make your account safer again by undoing this change at https://www.google.com/settings/security then switching to apps made by Google such as Gmail to access your account.

If you did not make this change
Please recovery your account by clicking the button below. Whoever made the change knows your password; we recommend that you change it right away.

Recovery account

Sincerely,
The Google Accounts team

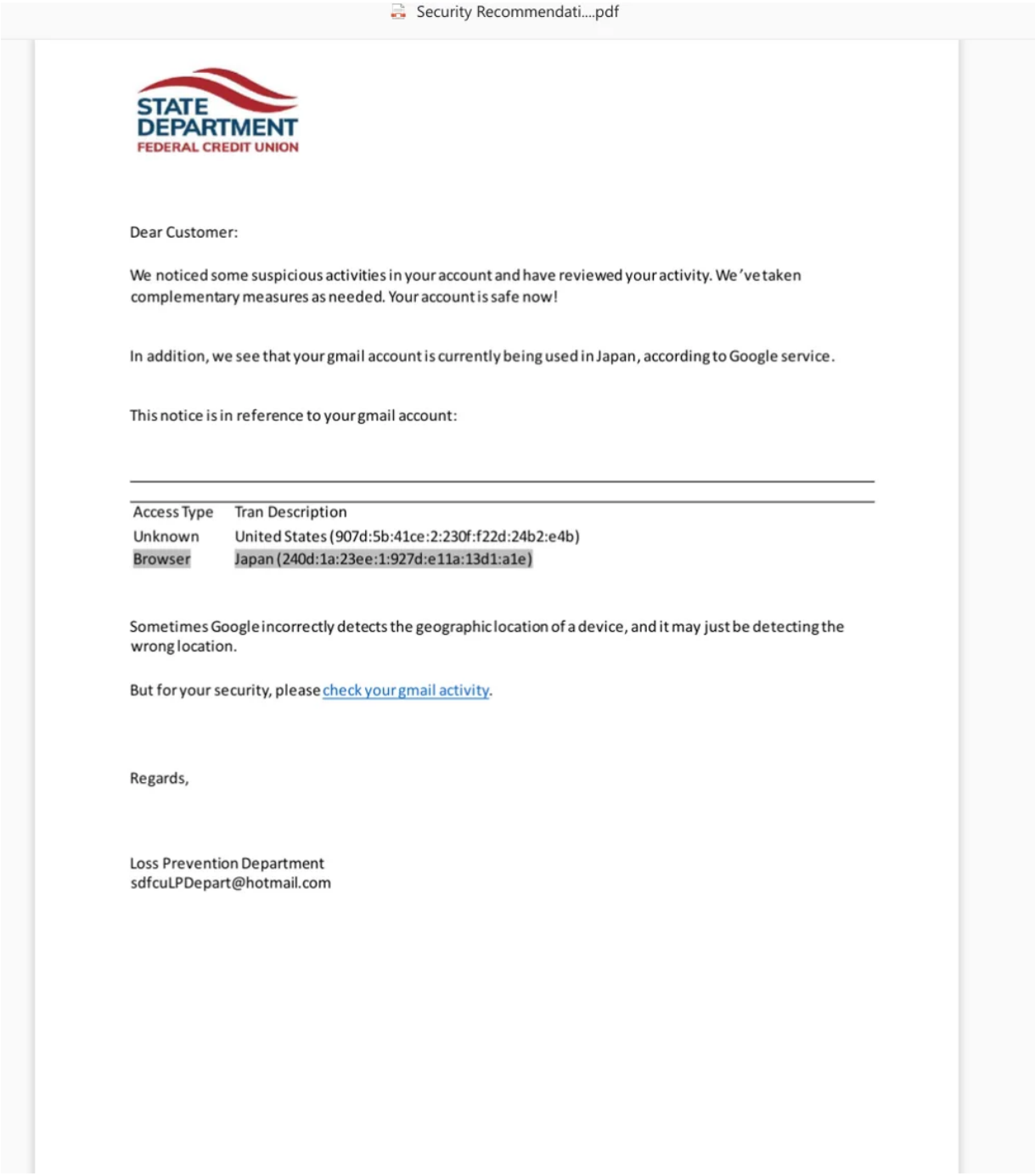
This email can't receive replies. For more information, visit the Google Accounts Help Centre.

You received this mandatory email service announcement to update you about important changes to your Google product or account.

@ 2015 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Example from 2015 of an ARCHIPELAGO phishing email

One example of ARCHIPELAGO's shifting phishing techniques is a campaign in late 2022 where they sent links to a benign PDF file hosted in OneDrive. The PDF claimed to be a message from the State Department Federal Credit Union notifying customers they detected malicious logins from their Google Account and that the customer should click the link in the PDF to verify activity from their Gmail account. If clicked, the link directed recipients to a phishing page. ARCHIPELAGO created unique PDFs for each recipient so that when the recipient clicked, the phishing page was pre-populated with the recipient's email address.

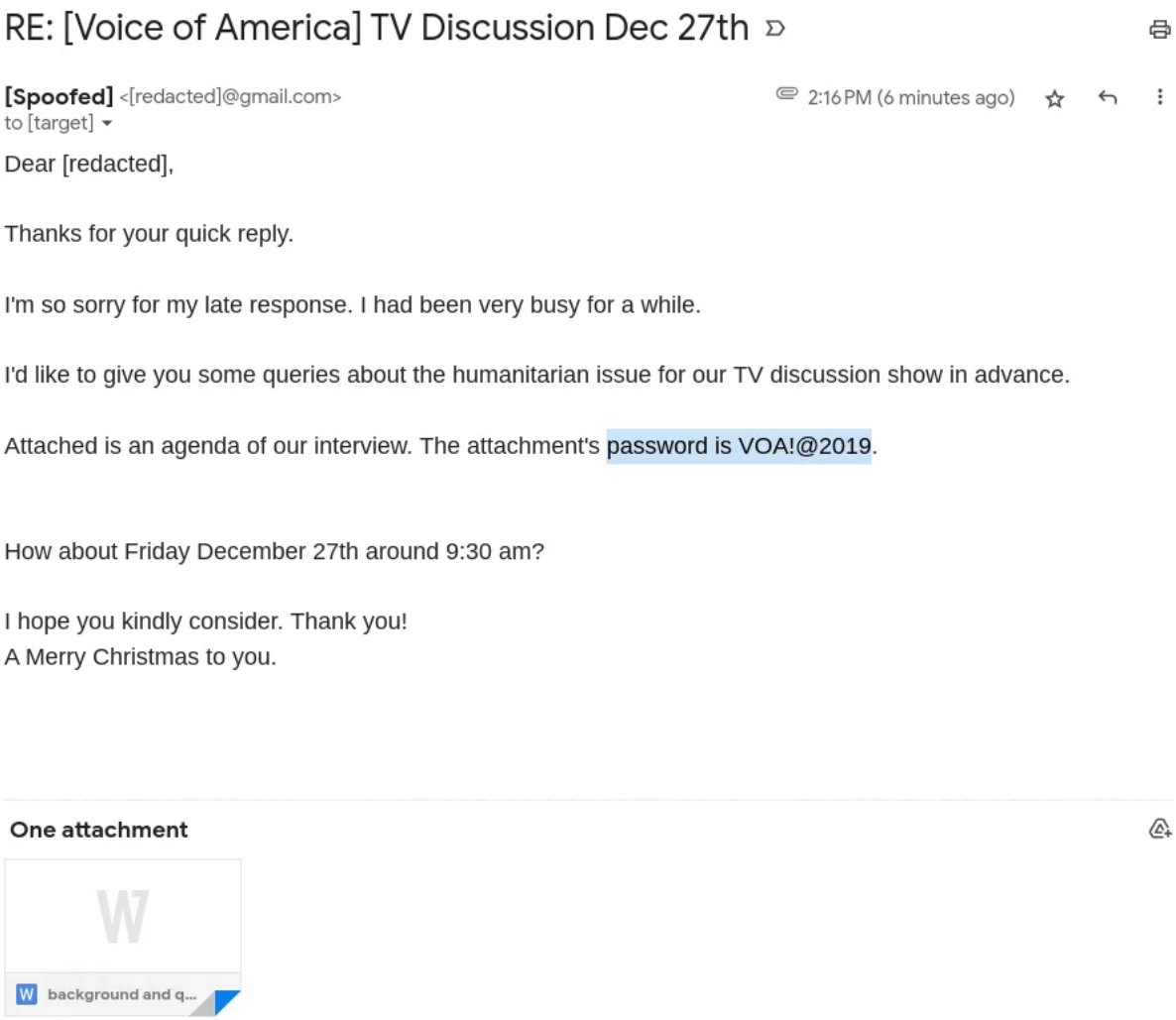


ARCHIPELAGO used legitimate cloud storage services to host benign PDFs with phishing links inside

By placing the phishing link inside a benign PDF hosted on a legitimate cloud hosting service, ARCHIPELAGO was likely trying to evade detection by AV services that do not scan links inside files.

Malware operations

For several years, ARCHIPELAGO focused on conducting traditional credential phishing campaigns. More recently, TAG has observed ARCHIPELAGO incorporate malware into more of their operations, including efforts to evade detection and develop novel malware techniques. To protect their malware from AV scanning, ARCHIPELAGO commonly password-protects their malware and shares the password with recipients in a phishing email.



ARCHIPELAGO phishing email with a password-protected attachment. The password for decrypting the attachment is included in the body of the phishing email.

Encoding malware payloads and commands in Drive file names

ARCHIPELAGO has experimented with their malware over time, including using novel malware delivery techniques. In 2020, they began testing a then-new technique with files they hosted on Google Drive. ARCHIPELAGO encoded malicious payloads in the filenames of files hosted on Drive, while the files themselves contained zero bytes of content. They also used Drive file names for C2, placing encoded commands in file names. Security researchers at Huntress and IssueMakersLab publicly reported on this technique.

Google took action to disrupt ARCHIPELAGO's use of Drive file names to encode malware payloads and commands. The group has since discontinued their use of this technique on Drive.

Malware packaged in ISO files

ARCHIPELAGO has also attempted to deliver malware via Drive using ISO files, a file format that has gained popularity among threat actors ranging from government-backed attackers to financially motivated groups. In one case TAG recently examined, ARCHIPELAGO sent a phishing email with a Drive link to an ISO file, Interview_with_Voice_of_America.iso. The ISO file contained a ZIP, which, in turn, contained a password-protected document. When decrypted, the document installed VBS-based malware related to BabyShark.

Malicious Chrome Extensions

ARCHIPELAGO has also used malicious Chrome extensions in combination with phishing and malware. The earliest versions of these extensions, reported as STOLEN PENCIL in 2018, included functionality to steal usernames,

passwords and browser cookies. They were delivered via phishing emails with a link that directed recipients to a lure document that prompted users to install the malicious Chrome extension. Google has since introduced several changes to the Chrome extension ecosystem, including enhanced transparency through the Chrome Web Store and Manifest V3, that effectively disrupt threat actors from distributing malicious extensions like STOLEN PENCIL via the Chrome Web Store. In 2018, Chrome also made improvements to the extension review process by making extensions that request powerful permissions subject to additional compliance review while also conducting ongoing monitoring of extensions that use remotely hosted code.

More recently, ARCHIPELAGO has attempted work-arounds to install a new malicious Chrome extension known publicly as SHARPEXT. If successfully installed on a user system, SHARPEXT can parse emails from active Gmail or AOL Mail tabs and exfiltrate them to an attacker-controlled system. As a result of improved security in the Chrome extension ecosystem, ARCHIPELAGO must now complete several additional steps to install the extension, including first successfully installing malware on the user system and then overwriting the Chrome Preferences and Secure Preferences files to allow the extension to run.

Protecting against advanced threats

TAG, in partnership with Mandiant and other security teams across Google, is committed to our mission of understanding and countering advanced threats. We apply our research to ensure Google's products are secure and our users are safe. For individuals at high risk of this activity and other serious threats, Google provides advanced security resources, including Enhanced Safe Browsing and the Advanced Protection Program. When these tools are used in combination with Google's Security Checkup, they provide the fastest and strongest level of protection against serious threats.

POSTED IN:

- Threat Analysis Group