CLCT

WILLIAM & MARY
LAW SCHOOL

Cybersecurity and Information Security Newsletter

Issue 26 | June 12, 2023

Table of Contents

Daniel Shin, research scientist with the Commonwealth Cyber Initiative (CCI) Coastal Virginia region, wants to hear from you! Submit any cybersecurity and information security news items or request related topics, via e-mail to dshin01@wm.edu.

This newsletter supports the mission of CCI. To learn more about CCI, including upcoming events, funded research, and news, please visit cyberinitiative.org.

Google Registry launches new top-level domains—.zip and .mov—raising cybersecurity concerns

On May 3, 2023, Google Registry (Google's domain name registry, which is responsible for managing top-level domains) announced the availability of eight new top-level domains for private use purchase. Top-level domain (TLD), indicated by the text following the period of a domain name, often refers to the website's type. (e.g., commercial, non-profit, or government website) *What is a top-level domain (TLD)?*, available here. For example, the TLD for "Google.com" is ".com," which is commonly used by commercial websites. Generally, websites use the following common TLDs: ".com," ".net," and ".org."

A domain registry is an organization tasked with managing top-level domain names, including creating domain name extensions, setting rules for domain name ownership, and working with domain registrars to sell domain names to the public. *What is the difference between a registry, registrar and registrant?*, available here.

Google Registry's eight new TLDs include ".dad," ".phd," ".prof," ".esq," ".foo," ".zip," ".mov," and ".nexus." Although it may not have intended to broaden the cyber attack opportunities through its expanded TLD offerings, the availability of ".zip" and ".mov" domain names creates new opportunities for threat actors to commit novel phishing campaigns that can lead to substantial cyber attacks.

Prior to Google Registry's new TLD offerings, ".zip" and ".mov" were commonly understood as file extensions for compression files and movie files, respectively. By allowing anyone to purchase domain names ending in either ".zip" or ".mov," threat actors can craft new phishing campaigns (explained below) that disguise web addresses as file names, which can lead to cyber victims downloading inadvertently malicious code to their systems.

As an illustration, please visit (by clicking or typing the following without the proceeding period on a web browser) coverletter.zip. Although the text may appear to refer to a common zip compression file containing a cover letter, this text is also a legitimate web address that can be hyperlinked for anyone to visit. The "coverletter.zip" domain, owned by this newsletter's writer Daniel Shin, illustrates the potential dangers of tricking users into accessing a file when, in fact, the text is interpreted as a web address.

Phishing Illustration

Using a ".zip" or ".mov" domain names, threat actors can create clever phishing campaigns that bypass email attachment malware scanners. Phishing is a social engineering attack where a threat actor poses as a trusted individual or organization to lure a victim into providing sensitive information or performing actions that compromise the victim's computer system. *Phishing [CISA]*, available here. This section presents a hypothetical scenario where a threat actor takes advantage of the ".zip" TLD to infiltrate an organization's IT system.

Given that phishing attacks are easy to initiate and have a certain level of success, the hypothetical threat actor plans to target unsuspecting employees of the target organization to download and execute inadvertently the threat actor's malware using a phishing email.

Most organizations employ automated malware scanning systems that check all inbound e-mail attachments, so threat actors are commonly forced to consider other means to send the malware into target IT systems.

Taking advantage of Google Registry's new TLD offerings, the hypothetical threat actor purchases the domain name "annual-safety-drill-slides.zip." (Note, this is a hypothetical scenario, and the domain name may have been purchased by another without malicious intentions.) Then, she creates a website under the new domain name and sets the webpage to trigger automatically a download prompt whenever someone visits the website. If any website visitor accepts the prompt and downloads the file, the threat actor's malware is transmitted immediately to the visitor's computer.

After setting up the download website, the threat actor drafts a phishing email that appears to have come from the organization's human resources department. The phishing email asks urgently all employees to open the "attached" zip file and review the slides or face potential administrative penalties. Although the threat actor is not able to attach directly the malware due to the organization's email attachment scanners, she instead creates a hyperlink to "annual-safety-drill-slides.zip" that appears visually like an email attachment using button graphics mimicking Microsoft Outlook's interface.

When the phishing campaign begins, some employees mark the phishing email as spam email due to obvious signs (e.g., spelling and grammar mistakes) indicating the email is spam. However, statistically some, even if only a few, employees are likely to misidentify the email as legitimate and click on the attachment-looking hyperlink to the ".zip" website. Knowing that the organization employs email attachment safety measures, the unsuspecting employee downloads the file, mistaking it as an email attachment that has been scanned by the system. Once the employee opens the file, the malware activates and spreads throughout the organization's systems.

This phishing illustration could have been thwarted by a more robust defense-in-depth approach by the organization, such as having an anti-malware scanner that checks all downloaded files, which may have alerted the employee not to open the file in the first place. But, it also highlights the potential user error of misinterpreting a web address as a file name, which broadens the threat actors' opportunities to deceive cyber victims.

Analysis

The Internet Corporation for Assigned Names and Numbers (ICANN) is a U.S.-based non-profit entity that is responsible for regulating and providing technical coordination of the Internet's domain name system, which includes regulating how domain names are created and distributed among stakeholders. *ICANN [National Telecommunications and Information Administration]*, available here. It is not clear whether ICANN or Google Registry performed any security impact assessments resulting in offering TLDs that appear clearly to be mistakable as file extensions. But many in the cybersecurity community have raised concerns about the foreseeable impact of ".zip" and ".mov" TLDs may have in bolstering threat actor's efforts in mimicking legitimate web addresses.

For example, security researcher Bobby Rauch illustrated another malicious phishing technique using the following similar-looking URLs:

1. https://github.com/kubernetes/kubernetes/archive/refs/tags∕@v1271.zip
2. https://github.com/kubernetes/kubernetes/archive/refs/tags/v1.27.1.zip

Although both web addresses look very similar, the first URL is a potential phishing URL that will direct the user to the domain name "v1271.zip" while the second address will download a zip file from "github.com," a popular code repository owned by Microsoft. *Google pushes .zip and .mov domains onto the Internet, and the Internet pushes back [Ars Technica]*, available here (citing *The Dangers of Google's .zip TLD*, available here.).

Given that many large organizations and other commonly-used websites have not migrated to ".zip" or ".mov" TLDs, blocking access to all websites with the ".zip" or ".mov" domain names may be the best proactive solution to preventing phishing attacks relying on these TLDs.

Blocking ".zip" and ".mov" TLDs using an adblocker for web browsers

To block all ".zip" and ".mov" domain names using uBlock Origin, a free adblocker for web browsers:

1. Install uBlock Origin for your web browser. *uBlock Origin*, available here.
2. Open the web browser, click on the uBlock Origin icon on the top right side of the browser window, and click "Options."
3. Select the "My filters" tab.
4. In the text field, add the following lines:
   ||zip^
   ||mov^
5. Click the "Apply changes" button to save the filter.

Thereafter, uBlock Origin will block all connections destined to any web addresses ending in ".zip" or ".mov" TLDs, which protect users if someone clicks accidentally on a malicious hyperlink using these types of web domain addresses. *See Can we block TLDs? [Reddit]*, available here.

FBI warns of malicious actors using deepfakes to facilitate Sextortion Schemes

On June 5, 2023, the Federal Bureau of Investigation (FBI) published a public service announcement (PSA) to warn the public of malicious actors creating and circulating deepfakes of victims for the purposes of harassing victims or committing sextortion schemes. *Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes [FBI] (FBI PSA)*, available here. Deepfakes are realistic but fake synthetic media created using generative AI. *See New Text-to-Image AI Model allows users to produce pornographic and other controversial content [Cybersecurity and Information Security Newsletter Issue 22]*, available here. Sextortion refers to coercing a minor into providing sexually explicit media of themselves and then threatening to share the media publicly, including to family and friends. *See Sextortion [FBI]*, available here.

According to the PSA, there has been an increase in sextortion victims who reported the use of fake images or videos synthesized using media (1) made available from the victims' social media pages and other online websites, (2) captured during video chats, or (3) "provided to the [threat actor] upon requests." *FBI PSA, supra*. Once the threat actor synthesizes fake images or videos of the victim, the threat actor typically demands either payment from the victim (if the victim fails to provide payment, the threat actor will threaten to share synthesized media with family and social media friends), or the victim sending real sexually themed images or videos that customarily is later used in further extortion.

The FBI recommends applying best practices to social media usage and taking extreme care in monitoring children's online activity and sharing children's photos and videos on social media networks. The PSA also showcases the National Center for Missing and Exploited Children's **Take It Down**, which is a free service that helps victims to remove or stop the online sharing of nude, partially nude, or sexually explicit media that was taken while the victim was under 18 years old. *Take It Down*, available here.

Analysis

The democratization of easy-to-use AI technologies ensures open access to cutting-edge technology for the public and provides the impetus for AI-driven innovation by the open-source community. Deepfakes programs have incorporated publicly available generative AI models to help users synthesize realistic but fake media. Although some users produced deepfakes for humorous or other experimental content, others commonly create sexually explicit media depicting an individual, often without consent. Creating deepfakes became easier as deepfakes software became more user-friendly and online websites specializing in deepfakes creation started to emerge publicly.

One legal means to discourage the creation of unconsented deepfakes is to pass legislation making it unlawful explicitly to create and transmit unconsented sexual or other types of media of another, regardless of how they were created. For example, Virginia provides victims of unconsented sexual media (including deepfakes) the right to sue those who created or disseminated such media. *Va. Code Ann. § 8.01-40.4 (2017)*, available here. Such statutes may provide effective deterrence of the creation and transmission of unconsented deepfakes of individuals, though admittedly they provide more limited deterrence against threat actors located abroad.

Legally and policy-wise, there needs to be a clear consensus as to when harm occurs in situations involving deepfakes. For example, the harm of deepfakes used to spread disinformation on social media may occur when other unsuspecting individuals receive AI-generated disinformation and recognize it as fact. In contrast, the harm arising out of unconsented deepfakes depicting sexual acts—arguably—is immediate when threat actors create and spread repulsive media. Based on when harm occurs, policymakers have the opportunity to design targeted legislation to criminalize foreseeably dangerous acts pertaining to deepfakes.

Ultimately, the FBI's sextortion notice showcases the importance of applying best practices for sharing personal data on the web, and it serves as a reminder of how online sexual predators continue to explore cutting-edge technology to commit crimes.