Mobile Browser Hijacker Attempts to Social Engineer Users to Install a Potentially Unwanted Program (PUP)

Executive Summary

Browser hijacking is a common technique leveraged by cybercriminals to social engineer users into downloading malware to their device. In some cases, these scams push trojans, ransomware and other malware. This occurs when a malicious webpage—or more likely, a malicious ad on an otherwise legitimate webpage—takes over the web browser. It is likely that the end user is not at risk after seeing this pop-up on their mobile device as long as they did not proceed to install the potentially unwanted program (PUP) to their device. However, it is possible that browser data is sent to an attacker when a victim navigates to these sites.

Report

On 12 May 2020 HC3 analysts investigated a suspicious domain that resulted in a pop-up on an iOS device from the domain goingapp[.]xyz. The pop-up claims to be an Apple Security message that states "(3) Viruses has been detected on your iPhone and battery has been infected and damaged. If you do not remove this malware now, it may cause more damage to your device. How to fix this: Step 1: Tap the button below & install the recommended VPN and virus protection tool free from the AppStore. Step 2: Run the app, follow on screen instructions to...," as shown in Figure 1. According to the screenshot, the potential incident occurred on 10 May 2020.

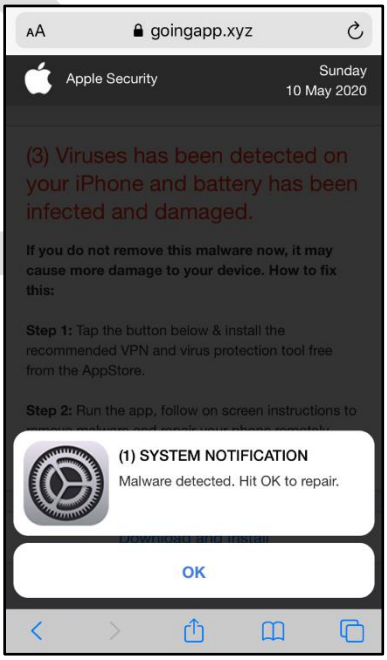

Figure 1. Screenshot of iOS device with pop-up from goingapp.xyz claiming viruses have been detected on the device and attempts to social engineer user to install a potentially unwanted program (PUP).

Analyst Comment

This appears to be a iOS scam and browser hijacking that attempts to trick users to installing a Potentially Unwanted Program (PUP) to their mobile device. According to PC Risk, Goingapp[.]xyz is similar to other scams hosted on greacore[.]com, apple-warning[.]com, and apple-online-guard[.]com. These scams claim the user's device is infected with viruses to social engineer them into installing an unwanted program or app. It is common that these sites are navigated to in the form of a browser redirect after a user accidentally clicks on a malvertisement, or malicious advertisement, on a legitimate webpage.

Technical analysis of domain goingapp[.]xyz on VirusTotal indicates Anti-Virus (AV) detection was marked as "Clean" with a community score of 0/84. HybridAnalysis rated this domain with "no specific threat" after analysis in a Windows environment. However, Forcepoint ThreatSeeker marked this domain as Suspicious. The domain resolved to the IP address 165.227.103[.]248 which geo-locates to the United States and is hosted with DigitalOcean, a legitimate cloud infrastructure provider headquartered in New York City. The domain was registered on 25 April 2020 according to WHOIS records from RISKIQ and does not include any registration information to provide indicators related to the individual or group operating the site. Overall, this domain is **suspicious** although no evidence of malware was identified being transferred to users simply by visiting the website. However, further attacks may occur if the user installs a PUP.

It is possible that websites like this gather browsing data from the victim such as IP addresses, geolocations, entered search queries, addresses of visited pages, and more. They can be designed to collect sensitive information which could be sold to third parties (potentially cyber criminals) who would then misuse it to generate revenue in other ways. **It is important that the end user confirm that no unauthorized or unwanted programs were installed to the device as a result of this pop-up. Some recommendations to clear this browser hijack from a user's device include clearing the browser's cache, disabling JavaScript, and using an external link to force open a new window.**

References

PC Risk, "How to uninstall apps that open pages like goingapp.xyz?" (29 April 2020)
https://www.pcrisk.com/removal-guides/17630-goingapp-xyz-pop-up-scam-mac
SensorsTechForum, "Goingapp.xyz Ads Removal Guide" (23 April 2020)
https://sensorstechforum.com/goingapp-xyz-ads-removal/
HowToRemoveGuid, "Goingapp.xyz " (22 April 2020)
https://howtoremove.guide/goingapp-xyz-virus/
VirusTotal, "Detection for goingapp[.]xyz" (accessed 12 May 2020)
https://www.virustotal.com/gui/domain/goingapp.xyz/detection
Bloomberg, "DigitalOcean LLC Company Profile" (accessed 12 May 2020)
https://www.bloomberg.com/profile/company/0852730D:US
RiskIQ, "goingapp[.]xyz search results" (accessed 12 May 2020)
https://community.riskiq.com/search/goingapp.xyz/whois
HybridAnalysis, "Sandbox results for hxxp://goingapp.xyz/" (accessed 12 May 2020)
https://tinyurl.com/y8crgwyw
Mac Observer, "Three Ways to Fix a Safari Browser Hijack in iOS 11" (24 Jan 2018)
https://www.macobserver.com/tips/how-to/fix-safari-hijack-browser-hijack-ios-11/