Published on *The National Law Review* https://natlawreview.com

Ankura CTIX FLASH Update - November 29, 2022

Article By:

Ankura Cyber Threat Investigations and Expert Services

Ransomware/Malware Activity

Threat Actors Exploiting Trending TikTok Challenge to Deploy Malware

Researchers at Checkmarx have identified a trending TikTok challenge that is prompting users to download information-stealing malware via Discord. TikTok is a video hosting service owned by ByteDance, a Chinese internet technology company, that has over 1 billion monthly active users and has been involved in various controversies for its privacy policy throughout recent years. A TikTok trend, called the "Invisible Challenge" which uses a video effect called "invisible body" to conceal the users' supposed undressed bodies, is currently being exploited by threat actors. The special effect is claimed to produce a blurred and contoured image of a person. Researchers have identified actors posting their own videos with links to malicious software, called "unfilter", that will supposedly remove the TikTok filter in question. As of late November 2022, the actors' videos have reached over 1 million views and the GitHub repository hosting the software code has been listed in GitHub's daily trending projects. The instructions to obtain the "unfilter" software prompts the user to join a Discord server. Once a user joins, various videos can be viewed as false proof of the filter being legitimate and a bot account prompts the user to star the actors' GitHub repository. When the “unfilter” software is run, it deploys "WASP" stealer malware, which is hidden inside malicious Python packages. Indicators of compromise (IOCs) concerning this latest campaign can be viewed in Checkmarx's report linked below, and CTIX analysts will continue to monitor campaigns exploiting social media platforms.

- The Record: Malware Via TikTok Article
- Medium: Checkmarx Report

Threat Actor Activity

Black Basta Unveils New Campaign Targeting United States Companies with Qakbot Malware

Black Basta threat actors have recently launched a new malicious social engineering campaign targeting United States corporations. Known for their double extortion tactics, Black Basta has been one of the larger threat groups emerging in 2022. Recently, the group was linked to the FIN7 cybercriminal organization after indicators from a previous attack overlapped with known FIN7

infrastructure. In the recent campaign, Black Basta threat actors are utilizing the Qakbot malware as the point-of-compromise in their attacks, capable of moving laterally throughout the victims' network. Qakbot is a banking trojan used to primarily steal financial data, including but not limited to credential pairs, keystrokes, and browser information. Several scenarios from this campaign have highlighted fast moving attacks, typically gaining access within two (2) to three (3) hours and deploying ransomware payloads in twelve (12) hours and locking out victims from their own network by disabling DNS protocols. After the attack, Black Basta actors will demand a significant ransom from the victim, using the stolen data as leverage in negotiations. Thus far, Black Basta has hit at least ten (10) corporations in this campaign and is likely to continue to in the coming weeks. CTIX continues to monitor threat actor activity worldwide and will provide additional updates accordingly.

- Dark Reading: Black Basta Article
- CyberReason: Black Basta Article

Vulnerabilities

Google Patches Critical Zero-Day Vulnerability on Thanksgiving Day

On Thanksgiving Day 2022, Google released an emergency Chrome browser update to patch an actively exploited critical zero-day vulnerability. The flaw, tracked as CVE-2022-4135, is a Google Chrome GPU heap buffer overflow vulnerability. When exploited, this vulnerability could allow a remote attacker to compromise the renderer process by performing a sandbox escape via a maliciously crafted HTML page. If successfully exploited, the threat actor could bypass security mechanisms, execute arbitrary code, and create denial-of-service (DoS) conditions in the Chrome browser, leading to system crashes. The flaw was first reported to Google by Clement Lecigne, a member of their own Threat Analysis Group, who observed the active exploitation of the flaw, leading to a patch release two (2) days later. At this time, there are not many details about the specifics of the exploitation, as Google is withholding the information to allow as many Chrome users as possible to update their browsers. Once the details of the exploit or a proof-of-concept (PoC) is released, unsophisticated threat actors will be scanning for vulnerable systems in an attempt to exploit as many targets as they can. CTIX analysts urge all Chrome users to verify that they are running version 107.0.5304.121 for Mac and Linux, and version 107.0.5304.121/.122 for Windows.

- The Hacker News: CVE-2022-4135 Article
- Google: CVE-2022-4135 Patch Advisory

National Law Review, Volume XII, Number 334