Office of the CHIEF INFORMATION SECURITY OFFICER State of Texas

Threat Actors spoof collaboration tools and related domains to target remote workforce amid COVID-19 pandemic

03/31/2020

Summary

On March 30, 2020, security vendor Checkpoint reported on the rise of newly registered Zoom-themed domains being leveraged for malicious purposes.

Zoom is a popular videoconferencing software company that provides its customers with a cloud-based communication platform to facilitate audio and video conferencing, online meetings, instant messaging, and collaboration via mobile, desktop, and telephone systems. Due to the current ongoing COVID-19 crisis, there has been an increased transition of workplaces to equip employees to work remotely from their homes. An effect of this transition is the increased reliance on remote collaboration and communication platforms such as Zoom, Microsoft Teams, Google Classroom, etc.

The increase in number of newly registered Zoom-themed phishing and malicious domains is indicative of threat actors attempt to abuse the most popular trends and platforms as part of their ongoing attacks.

Additional Details

According to researchers at Checkpoint, they have tracked the creation of 1,700 new domains with the keyword "Zoom" since the beginning of the year, as an effort to look for potential phishing sites. A quarter of said domains having been created within 7 days prior to reporting and 4% of all Zoom-themed domains have been discovered to contain suspicious characteristics. These domains can act as phishing sites as employees use their browsers to join meetings or can be used to host malware and lure unsuspecting users to download and install them on their systems or mobile devices.

Checkpoint researchers also observed new phishing websites that impersonated the official Google Classroom site with domains such as "googloclassroom[.]com" and "googieclassroom[.]com". The researchers also observed malicious executable files masquerading as remote collaboration tools such as "zoom-us-zoom_##########.exe" and "microsoft-teams_V#mu#D_##########.exe" (where # represents various digits), which upon execution will install "InstallCore", which is a potentially unwanted application (PUA) and can result in installation of other third-party applications, browser plugins, or even malware on the compromised system or device. InstallCore on Windows operating systems is known to disable User Access Control (UAC), add files to be launched on startup, install browser extensions, and change browsers configuration and settings, essentially lowering browser security.

For additional details, visit the Checkpoint post: https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/ 03/30/2020

DIR.TEXAS.GOV

Assistance/Feedback/Questions?

Office of the Chief Information Security Officer
DIRSecurity@dir.texas.gov
Texas Department of Information Resources

Transforming How Texas Government Serves Texans