DigiKnow

CYBER SECURITY DEPENDS ON YOU

NEW THREATS - TikTok and Malicious Use of Legitimate Remote Monitoring

February 2023| Issue 2023:3

GROWING SECURITY CONCERNS LEAD TO TIKTOK BAN FOR STATE NETWORK AND DEVICES

TikTok, an algorithm-based, short-form video sharing social media platform, exploded in popularity over the past several years, reaching one billion monthly active users in September 2021. It's wildly popular with teenagers — a 2022 Pew Research Center survey found two-thirds of American teenagers aged 13-17 use the app.

Numerous federal and state entities have issued warnings regarding national security concerns with TikTok which is owned by the Chinese company ByteDance. The federal government banned TikTok on government-owned devices in December 2022 and numerous states have since followed suit.

Chief Information Officer, Jason Clarke informed all State of Delaware Computing Network users on January 23, 2023, that **TikTok will not be permitted on state-owned devices or the network.** Enforcement of the ban began earlier this month.

TikTok vulnerabilities identified include:
• Collection of keystrokes of users, screen captures, and access to data from the phone's clipboard.
• Harvesting data that may include passwords, location, and other sensitive information. This could include information from other apps used on the device, like email and text messages.
• State-owned electronic devices may enable the Chinese government to obtain confidential, private, or other data from Delaware agencies or employees.

SMISHING ALERT

This smishing text below has been making the rounds on Delaware-based smart phones. Smishing is a form of phishing in which an attacker uses a compelling text message to trick targeted recipients into clicking a link and sending the attacker private information or downloading malicious programs. Be on the lookout for suspicious texts like this one and **DO NOT REPLY VIA PHONE OR TEXT.**

Joint Cybersecurity Advisory (CSA) Malicious Use of Remote Monitoring Software

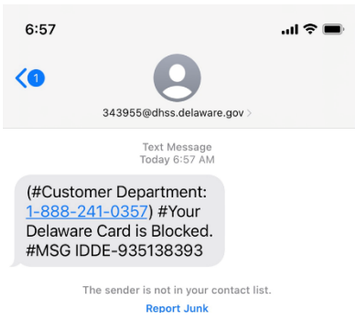
The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) released a joint Cybersecurity Advisory (CSA) to warn network defenders about malicious use of legitimate remote monitoring and management (RMM) software. In October 2022, CISA identified a widespread cyber campaign involving the malicious use of legitimate RMM software. Specifically, cyber-criminals sent phishing emails that led to the download of legitimate RMM software—ScreenConnect (now ConnectWise Control) and AnyDesk—which the actors used in a refund scam to steal money from victims' bank accounts.

Although this campaign appears financially motivated, the authoring organizations assessed that it could lead to additional types of malicious activity. For example, the actors could sell victim account access to other cyber criminals or advanced persistent threat (APT) actors. This campaign highlights the threat of malicious cyber activity associated with legitimate RMM software: after gaining access to the target network via phishing or other techniques, malicious cyber actors—from cybercriminals to nation-state sponsored APTs—are known to use legitimate RMM software as a backdoor for persistence and/or command and control (C2).

Much of this advisory delves into the more technical details of the malicious use of RMM software and how the cyber criminals can bypass many software controls and administrative privilege requirements. What is important to typical network users to understand is that these bad actors use Phishing emails as their primary method of launching attacks.

Since at least June 2022, cybercriminal actors have sent help-desk-themed phishing emails to employees' personal and government (or business) email addresses. The emails either contain a link to a "first-stage" malicious domain or prompt the recipients to call the cybercriminals, who then try to convince the recipients to visit the first-stage malicious domain.

One example of an actual phishing email was purportedly from Best Buy's Geek Squad, telling the recipient their Geek Squad subscription was being renewed. It informed the supposed "customer" that if they had not authorized this transaction, to immediately call an 800 number to cancel the payment. Even though it was a phishing attempt, the bogus email told the customer NOT to reply to the email, but only to call the 800#. Cyber criminals were awaiting calls at the supposed customer service number, and from there, the phishing target would be convinced to take further action at their direction (such as providing banking/credit card details).



Over three billion phishing emails are sent daily, according to email security firm, Valimail. One reason why email remains such a common attack vector is because of the rise of remote working. Employees are dealing with an increase in business communications being conducted over email, while the reality of working from home means that it's harder for some to ask a coworker if an email is legitimate.

An informed, cyber-aware workforce is the first line of defense for preventing campaigns such as the malicious use of legitimate remote monitoring software. No longer are phishing emails limited to attempts to gather personal information, they are increasingly methods of large scale criminal activity.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**