How RAT Malware Is Using Telegram to Evade Detection

bollyinside.com/articles/how-rat-malware-is-using-telegram-to-evade-detection/

February 12, 2022

This tutorial is about How RAT Malware Is Using Telegram to Evade Detection. Recently I updated this tutorial and will try my best so that you understand this guide. I hope you guys like this blog, ***How RAT Malware Is Using Telegram to Evade Detection***. If your answer is yes after reading the article, please share this article with your friends and family to support us.

Check How RAT Malware Is Using Telegram to Evade Detection

Malware is a collective term for any type of malicious software designed to harm or exploit programmable devices, services, or networks. Cybercriminals often use it to extract data that they can use to financially exploit their victims. This data can range from financial data to health records, personal emails and passwords; the possibilities of what kind of information can be compromised are endless. Digitization is increasing day by day and so are cyber attacks, scams and malware attacks. Although users take many security measures to protect themselves from such attacks, hackers find various ways to penetrate users' devices.

Now, cybersecurity researchers have issued an important warning to Telegram users: Devices and PCs are being hacked by Windows-based malware that spreads via fake Telegram Messenger app installers. Malware can hide from installed antivirus systems, steal

your data and download other malicious files to the system. In this way, many users may not know that their device is already infected. ToxicEye is a type of malware called a Remote Access Trojan (RAT). RATs can allow an attacker to remotely control an infected computer.

Malware that chats on Telegram

In early 2021, dozens of users abandoned WhatsApp and switched to messaging apps that promised more data security after the company announced it would share users' default metadata with Facebook. Many of those users turned to rival apps Telegram and Signal. According to us, Telegram was the most downloaded app in January 2021, with over 63 million installs. Telegram chats aren't end-to-end encrypted like Signal chats, and now Telegram has another problem: malware.

Software company Check Point recently discovered that malicious actors were using Telegram as a communication channel for a malware program called ToxicEye. It turns out that attackers can use some features of Telegram to interact with their malware more easily than through web-based tools. They can now mess with infected computers through a helpful Telegram chatbot.

What is ToxicEye and how does it work?

ToxicEye is a type of malware called a Remote Access Trojan (RAT). RATs can give an attacker remote control over an infected computer, which means that:

- steal data from the host computer.
- delete or transfer files.
- kill the processes running on the infected computer.
- hijack computer microphone and camera to record audio and video without user's consent or knowledge.
- encrypt files to extort money from users.

ToxicEye RAT is spread via a phishing scheme in which the targeted person receives an email with an embedded EXE file. When the targeted user opens the file, the program installs the malware on their device. RATs are similar to remote access programs that, for example, allow a technician to take control of your computer to fix a problem. But these programs sneak around without permission. They can mimic or be hidden within legitimate files, often disguised as documents or embedded in a larger file, such as a video game.

The chain of infection

- The attacker first creates a Telegram account, then a Telegram "bot", which can perform actions remotely through the app.
- This bot token is embedded in malicious source code.

- This malicious code is sent as spam, which is often disguised as something legitimate that the user can click on.
- The attached file is opened, installed on the host computer, and sends the information to the attacker's command center via the Telegram bot.

Final remarks: How RAT Malware Is Using Telegram to Evade Detection

I hope you understand this article, *How RAT Malware Is Using Telegram to Evade Detection*. If your answer is no, you can ask anything via the contact forum section related to this article. And if your answer is yes, please share this article with your friends and family to give us your support.

Related Articles