AlertsTFlower Ransomware Campaign

cyber.gc.ca/en/alerts/tflower-ransomware-campaign

CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Number: AL19-201
Date: 20 September 2019

Purpose

On 30 July 2019 a new variant of ransomware named TFlower was discovered. The Cyber Centre has become aware of this ransomware recently affecting the Canadian public.

Assessment

The initial infection vector for this malware appears to be through Remote Desktop services, and other infection vectors may include email spam and malicious attachments, deceptive downloads, botnets, malicious ads, web injects, fake updates and repackaged and infected installers. Once a malicious actor infects a system, they may attempt to move laterally across the network through tools such as PowerShell Empire, PSExec, etc.

The malware will initially contact a Command and Control(C2) server to indicate its readiness to encrypt the contents on the target system. It will then delete shadow copies and disable recovery features in Windows 10 and create persistence by adding a key in the logged in user's software registry hive. It will encrypt files and mark them by inserting the string "*tflower" at the beginning of the file but will not change the filename.

Finally the malware will update the C2 server and leave a ransom note named “!_Notice_!.txt” placed throughout the computer and on the Windows Desktop.

The Cyber Centre recommends that all system owners apply the latest security patches immediately, and that system users are reminded to be vigilant when following unsolicited links and opening unexpected document attachments in emails, even if they come from known contacts.

Suggested action

- Install the latest updates for the vulnerable operating systems.
- Disable Remote Desktop Services if not required. If required, closely monitor network traffic and the logs of any vulnerable systems for suspicious activity.
- Enable Network Level Authentication (NLA) on all currently supported versions of Windows. This is a partial mitigation which will prevent the spread of the malware. With NLA enabled, an actor would first need to have credentials to an account on the target system.
- Block TCP port 3389 on the firewall, if possible. This will prevent unauthorized access from the Internet.
- Never open attachments from unknown or unverified sources.
- Whitelist applications to prevent unauthorized applications from running.
- Use antivirus and ensure that it is diligently kept up to date.
- Minimize the number of users with administrative privileges and ensure users do not have privileges to install software on their devices without the authorization of an administrator.
- Disable macros for documents received via email.
- Follow the Government of Canada’s guidance to stay CyberSafe https://www.getcybersafe.gc.ca/index-en.aspx

References

CCCS Alert on Critical Remote Desktop Vulnerability: https://cyber.gc.ca/en/alerts/critical-microsoft-remote-desktop-vulnerability

Note to readers

The Canadian Centre for Cyber Security (Cyber Centre) operates as part of the Communications Security Establishment. We are Canada's national authority on cyber security and we lead the government's response to cyber security events. As Canada's national computer security incident response team, the Cyber Centre works in close collaboration with government departments, critical infrastructure, Canadian businesses and international partners to prepare for, respond to, mitigate, and recover from cyber events. We do this by providing authoritative advice and support, and coordinating information sharing and incident response. The Cyber Centre is outward-facing, welcoming partnerships that help build a stronger, more resilient cyber space in Canada.