Cyber Snapshot

Exploring and Assessing Current Topics

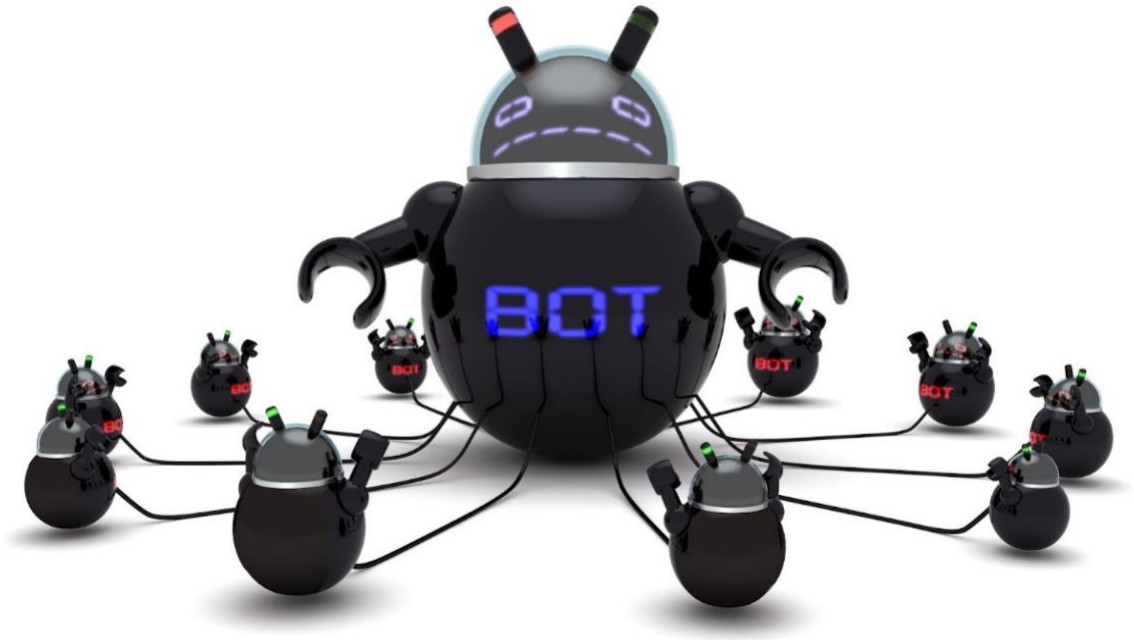
MICHIGAN CYBER COMMAND CENTER (MC3)

May 1, 2024
CS-04-24

UNLEASHING MALICE – THE DARK SIDE OF JAILBROKEN DEVICES

OVERVIEW:

In the realm of smartphones, tablets, smart devices, IoT (Internet of Things) and 'jailbreaking' – the process of exploiting flaws of a device to install software other than what the manufacturer has made available for that device – has been a topic of debate. The act itself may advertise or showcase that the device can work outside of what it was originally intended for and expand its capabilities. However, this act comes with significant risks that can compromise device security and user privacy. The act can expose the devices' security to a plethora of attacks and the device can be harnessed and controlled by bad actors.



THE ISSUE:

'Jailbreaking' circumvents the built-in security measures of the device. Without the security measures, users are more susceptible or able to download applications, 'hacks', 'tweaks' containing malware, spyware, or other harmful payloads. The malicious applications can steal personal data such as passwords and files, track user activities, flood other devices on the Internet with traffic, control hardware and software of the device (like a camera or other application), send out malicious commands, be used to support criminal activities, take control of the device remotely, putting anyone/everyone else that uses the Internet at risk.

Further, 'jailbreaking' a device sacrifices access to official software updates and support from the device manufacturer. The act of 'jailbreaking' a device comes at the cost of forfeiting critical security patches and bug fixed provided in the official updates. The 'jailbroken' devices become perpetually vulnerable to known security flaws, making them very easy targets of cyber-attacks and data breeches.

The 'jailbroken' device can become controlled by someone or even other malicious software that is outside the control of the correct user. With multiple devices under the control of a bad actor a large group of these devices can wreak havoc across cyberspace. This can 'harness' the victim user's resources (Internet, infrastructure, etc.) to further the bad actors' criminal activities or other maliciousness. The remote access can often be totally unknown by the victim user and might go undetected or often not detected until the remote access has been occurring for a significant amount of time.

The act of 'jailbreaking' alters and changes the core functionality of the device's operating system which can also lead to system instability and the degradation of system performance. Permanent damage can occur to the device as well.

'Jailbreaking' typically violates the end-user license agreement (EULA) and terms of service established by the device manufacturer. Users risk voiding their warranty and facing legal consequences for unauthorized modification of the device's software. Manufacturers could refuse to provide repair or replacement services for 'jailbroken' devices.

CONCLUSION:

While 'jailbreaking' a device or purchasing one may seem like a tempting endeavor, it comes with an inherent risk and consequences that cannot be ignored. From increased susceptibility to malware and exploits to the loss of official support and warranty coverage, the potential dangers of 'jailbroken' devices far outweigh the perceived benefits.

It is recommended that users purchase devices from legitimate sources and preform reliable research on those devices that are used on the Internet. Regular software updates and security checks are paramount. It is recommended that users do this especially with devices that have access to sensitive information and before connected to networks (like home Internet) prior to use.

ADDITIONAL RESOURCES:

For more information and additional resources, please visit www.michigan.gov/mc3.

To report a cyber incident to the MC3, please contact 1-877-MI-CYBER or mc3@michigan.gov.