



# Cyber News



Articles of Interest

MICHIGAN CYBER COMMAND CENTER (MC3)

August 15, 2019  
CN-11-2019

Cyber News is a collection of open source news articles meant to increase cyber situational awareness. These articles have been chosen based on their publication date and relevance to the cyber community. This product will be disseminated on a continual basis so that recipients can stay abreast of current cyber concerns and events.

**Capital One Data Breach Affects 106 Million Customers; Hacker Arrested (30 July)**

<https://thehackernews.com/2019/07/capital-one-data-breach.html>

**Pakistani Man Bribed AT&T Insiders to Plant Malware and Unlock 2 Million Phones (06 August)**

<https://thehackernews.com/2019/08/sim-device-unlocking-malware.html>

**Cerberus: A New Android 'Banking Malware for Rent' Emerges (13 August)**

<https://thehackernews.com/2019/08/cerberus-android-banking-trojan.html>

**New Hexane Group Targets Oil and Gas, Telco Providers (01 August)**

<https://www.bleepingcomputer.com/news/security/new-hexane-group-targets-oil-and-gas-telco-providers/>

**New SystemBC Malware Uses Your PC to Hide Malicious Traffic (01 August)**

<https://www.bleepingcomputer.com/news/security/new-systembc-malware-uses-your-pc-to-hide-malicious-traffic/>

**Beware of Emails Asking You to "Confirm Your Unsubscribe" Request (04 August)**

<https://www.bleepingcomputer.com/news/security/beware-of-emails-asking-you-to-confirm-your-unsubscribe-request/>

**New Bluetooth KNOB Flaw Lets Attackers Manipulate Traffic (13 August)**

<https://www.bleepingcomputer.com/news/security/new-bluetooth-knob-flaw-lets-attackers-manipulate-traffic/>

**Nation-State APTs Target U.S. Utilities with Dangerous Malware (02 August)**

<https://threatpost.com/nation-state-apt-target-u-s-utilities-with-dangerous-malware/146910/>

**Mass Spoofing Campaign Abuses Walmart Brand (06 August)**

<https://threatpost.com/mass-spoofing-campaign-walmart/146994/>

**State Farm Falls Victim to Credential-Stuffing Attack (08 August)**

<https://threatpost.com/state-farm-credential-stuffing-attack/147139/>

**Android Apps Containing Clicker Trojan Installed on over 100M Devices (10 August)**

<https://securityaffairs.co/wordpress/89675/malware/android-apps-clicker-trojan.html>

**WhatsApp Flaws Allow the Attackers to Manipulate Conversations (08 August)**

<https://securityaffairs.co/wordpress/89624/hacking/whatsapp-flaws-2.html>

**New Trickbot Variant Found Using Highly Obfuscated JS File for Propagation (06 August)**

<https://cyware.com/news/new-trickbot-variant-found-using-highly-obfuscated-js-file-for-propagation-6190a279>

**Attackers Leverage Tor Network to Operate C2 Servers of Mirai (01 August)**

<https://cyware.com/news/attackers-leverage-tor-network-to-operate-c2-servers-of-mirai-0a70898a>

*This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. This information is designated UNCLASSIFIED//TLP: WHITE and is shared in confidence. This document must not be reclassified in any way, in whole or in part. Further distribution of this information can occur without restriction.*