# CPIDER

## Cyber Patrol for Identification of Emergent Risks

### Fake adblockers caught 'cookie stuffing'

Google Chrome extensions posing as popular add blockers AdBlock and uBlock were discovered saving cookies in the web browsers to generate income from referral schemes. Although ad blockers provide a lot of useful features some of them have also been found to pose huge risks to user privacy through 'Cookie Stuffing' to generate revenue for developers. Google has removed the fake adblockers from Google Chrome Store. *(source: https://threatpost.com/malicious-ad-blockers-for-chrome-caught-in-ad-fraud-scheme/148591/)*

### North Korean hackers target ATMs in India

North Koreans hackers have been observed using a malware to target ATMs in India. The malware named ATMDtrack was first spotted in summer 2018. The malware attack has been attributed to a group of hackers known as Lazarus Group known to operate from North Korea. *(source: https://www.zdnet.com/article/new-north-korean-malware-targeting-atms-spotted-in-india/)*

## Mobile Phone Chargers as Hacking Tools

Simply charging your smartphone can lead to your data being stolen. The product, an iPhone charging cable designed by a hacker known as MG was showcased at Def Con, world's largest hacking conference. The cable is fitted with an extremely small Wi-Fi enabled implant and looks exactly like a legitimate iPhone charging cable. Once the cable is plugged in an iPhone, a hacker using a Wi-Fi network can use it to gain access to the iPhone. The hacker has claimed that similar technology can be implemented for any other type of charging cable. *(source: https://techcrunch.com/2019/08/12/iphone-charging-cable-hack-computer-def-con/)*

## Critical Flaw Detected in Internet Explorer

A flaw in the internet explorer has been identified leading Microsoft to release a security update for the browser. The vulnerability can be exploited to inject malware into the target computer. The flaw, which was discovered by Clément

## CCTV Cameras-A Potential Privacy Risk

Your own CCTV Cameras with access to the internet (using an IP addressing scheme) can be hacked to spy on you. This can not only lead to serious breach of privacy but can also be used to monitor network activity, capturing sensitive data like usernames and passwords or launching a malicious attack on the users system. Symantec's chief security expert has advised users to keep their camera software updated and to change usernames and passwords that come as default with the camera.

## Malware targets cloud security

A malware that targets cloud security has been identified by researchers at Palo Alto. Used by a hacking group known as 'Rocke' the malware raises serious concerns as people and organisations world over are increasingly shifting to cloud servers for data storage *(source:https://www.techrepublic.com/article/malware-can-now-evade-cloud-security-tools-as-cybercriminals-target-public-cloud-users/)*

**For online edition of CPIDER click www.jkpolice.gov.in/E-Crime**

Lecigne of the Google Threat Analysis Group is present in IE versions 9 to 11. *(source: https://threatpost.com/microsoft-internet-explorer-zero-day-flaw-addressed-in-out-of-band-security-update/148584/)*

## Right to be Forgotten to be limited to EU

The European Court of Justice has ruled that Google does not have to comply with General Data Protection Regulation (GDPR) of European Union pertaining to '*Right to be forgotten*' except in 28 EU countries. Right to be forgotten refers to the rights of individuals to have online references regarding them removed from search engines. Google has received 8,50,000 requests to remove links to about 3.3 million websites since 2014. *(source: https://www.theverge.com/2019/9/24/20881415/european-union-right-to-be-forgotten-worldwide-french-privacy-watchdog-eu)*

## Facebook removes thousands of apps over concerns of data security


Facebook has removed thousands of apps from its website amid concerns of data security. Although most of these applications were still in their testing phase, they were removed because of non-compliance to Facebook rules. These include apps like myPersonality, LionMobi and JedMobi some of which used to store user profile data on poorly secured sites. *(source: https://www.engadget.com/2019/09/20/facebook-developer-investigation-suspends-apps/)*

**A vulnerability in Rich Reviews-a plugin used by websites to collect user reviews has put around 16,000 WordPress sites in danger.** *(source: https://threatpost.com/unpatched-bug-wordpress-xss/148656/)*