InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Xiaomi cameras connected to Google Nest mistakenly sending video feed to other users
2. Chrome extension stealing crypto-wallet private keys
3. Malware attack on Landry's POS systems
4. Cisco has address several critical and high-severity issues.

23/12/2019

Introduction to InfoSec Weekly

InfoSec Weekly is a compilation of security related news feed that aims to update the readers about cyber security, cyber threats, malware attacks, new technologies and cyber security awareness every week. We primarily cover events and news related to offensive side of the Information Security such as hacking, password and sensitive information leakage, new vulnerabilities and important CVE ' s that can impact an individual or an organization. We also aim to provide defensive tactics to overcome known vulnerabilities that can protect organizations and individuals from any attacks.

Our main aim is to spread awareness regarding various cyber related threats.

About Us

We are a team of security enthusiasts with an aim to provide various Information Security Services to organizations. Our company aims to provide professional grade cyber security solutions for all your Information Technology infrastructures. Our team has been demonstrating penetration testing skills using methodologies such as OSSTMM, NIST and OWASP. We aim to help companies protect their valuable data from any internal or external threats. Our team members have been practicing their skills to detect and report vulnerabilities in a live environment. Organizations such as Google, Facebook, Twitter, Yahoo!, ebay, eset, bugcrowd, under armour, coinbase, CCM, etc have recognized our team members for reporting vulnerabilities and have helped these organizations from malicious users. Our team ' s professional work experience consists of various Government organizations, National and International based private organizations, INGOs, etc. Our Services ranges from VAPT, Incident Response, Information Security Training, Endpoint threat analysis, Cyber security consultant, etc.

1. Xiaomi cameras connected to Google Nest mistakenly sending video feed to other users

Description
Xiaomi's smart IP cameras have been found to be mistakenly sharing surveillance footage with other users without their permission. This issue seems to affect the cameras only when they are connected to Google's Nest Hub. It is assumed that a bug in the way Xaomi cameras communicate with Google Nest Hub is causing the issue. Google has temporarily disabled Xiaomi devices' access to its Nest Hub and has advised users to unlink their cameras from Google Nest Hub until a patch arrives.

Source	https://thehackernews.com/2020/01/google-nest-xiaomi-camera.html
Infected Technology	Xiaomi
Recommendation	To unlink their cameras from Google Nest Hub until a patch arrives.

2. Chrome extension stealing crypto-wallet private keys

Description	
Chrome extension called 'Shitcoin Wallet' has been caught injecting JavaScript code on web pages to steal passwords and private keys from cryptocurrency wallets and cryptocurrency portals. It allows users to manage Ether (ETH) coins and Ethereum ERC_{20}-based-tokens. However, Harry Denly, Director of Security at MyCrypto platform has discovered that the extension contains malicious code. Any funds managed by the extensions are at risk. The extension sends the private keys of all wallets created or managed through its interface to a third-party website called erc20wallet[.]tk. It also injects malicious JavaScript code when users navigate to well known cryptocurrency management platforms. This code steals login credentials, private keys and sends the data to the same third-party website.	
Source	https://www.zdnet.com/google-amp/article/chrome-extension-caught-stealing-crypto-wallet-private-keys/
Infected Industry	Google Chrome

3. Malware attack on Landry's POS systems

Description	
Landry's, a popular restaurant chain in the USA disclosed a malware attack on its point of sale systems that allowed cybercriminals to steal customers' payment card information. The malware searched for track data read from a payment card after it was swiped on the order-entry systems. It was designed to search and steal sensitive customer credit card data, including credit card numbers, expiration dates, verification codes and in some cases cardholder names.	
Source	https://www.landrysinc.com/CreditNotice/CANotice.asp
Infected Technology	Landry
Recommendation	To closely monitor their payment card statement for any unauthorized activity

4. Cisco has address several critical and high-severity issues.

Description
Dozen of vulnerabilities have been addressed in Data Center Network Manager (DCNM), one of the product of Cisco. Those vulnerabilities includes some critical flaws which could be exploited by attackers to bypass authentication and execute arbitrary actions with admin privileges on the vulnerable devices. Also those vulnerabilities includes high severity issues which could be exploited by an attacker with administrative privileges to execute arbitrary SQL commands on a vulnerable devices and also an attacker with admin rights to inject arbitrary commands on the underlying operating system.

Source	https://securityaffairs.co/wordpress/95930/security/cisco-dcnm-flaws.html
Infected Technology	Cisco
CVE Details	CVE-2019-15975 CVE-2019-15976 CVE-2019-15977

For any queries/recommendations:

Contact us: **whois@cryptogennepal.com**