June 29, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- Google Analytics Hacking
- Geo Vision Critical Bug and Backdoor found
- Docker Image containing Cryptojacking Malware
- Nvidia warns Windows gamers of serious Graphics Driver Bugs
- Credit card skimmer embedded in image metadata on e-commerce sites
- Twitter faced data breach of Business Account

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. Google Analytics Hacking

Description

Researchers reported that hackers are exploiting Google's Analytics service to steal credit card information from compromised e-commerce sites. Kaspersky, Sansec, and PerimeterX all published reports claiming that attackers are injecting data-stealing code onto the infected sites along with a Google Analytics tracking code for their own account. This allows the threat actors to exfiltrate payment information entered by customers, even when security policies are enforced. Kaspersky stated that it uncovered roughly two dozen infected websites across Europe, North America, and South America, that have been infected. The compromised e-commerce sites specialize in selling digital equipment, cosmetics, spare parts, and food products. The success of the attacks is contingent on e-commerce sites using Google's web analytics service for tracking visitors and have whitelisted the associated domains in their content security policy

Source	https://thehackernews.com/2020/06/google-analytics-hacking.html
Infected Technology	Google Analytics Service
Recommendation	Set CSP rules that restrict data exfiltration to other accounts

2. Geo Vision Critical Bug and Backdoor found

Description

Enterprise security firm Acronis said it discovered the vulnerabilities last year following a routine security audit of a Singapore-based major retailer. A Taiwanese manufacturer of video surveillance systems and IP cameras named Geo Vision, recently patched three of the four critical flaws impacting its card and fingerprint scanners that could've potentially allowed attackers to intercept network traffic and stage man-in-the-middle attacks. Malicious attackers can establish persistence on the network and spy on internal users, steal data — without ever getting detected. They can reuse your fingerprint data to enter your home and/or personal devices, and photos can be easily reused by malicious actors to perpetrate identity theft based on biometric data.

Source	https://www.bleepingcomputer.com/news/security/geovision-access-control-devices-let-hackers-steal-fingerprints/
Infected Technology	Geo Vision Surveillance cameras
CVEs	CVE-2020-3928, CVE-2020-3929, CVE-2020-3930
Recommendation	Update to the latest patches

3. Docker Image containing Cryptojacking Malware

Description

With Docker gaining popularity as a service to package and deploy software applications, malicious actors are taking advantage of the opportunity to target exposed API endpoints and craft malware-infested images to facilitate distributed denial-of-service (DDoS) attacks and mine cryptocurrencies. According to a report published by Palo Alto Networks' Unit 42 threat intelligence team, the purpose of these Docker images is to generate funds by deploying a cryptocurrency miner using Docker containers and leveraging the Docker Hub repository to distribute these images.

Source	https://unit42.paloaltonetworks.com/cryptojacking-docker-images-for-mining-monero/
Infected Platform	Docker Hub
Recommendation	check if they expose API endpoints on the Internet, close the ports

4. Nvidia warns Windows gamers of serious Graphics Driver Bugs

Description

Nvidia, Graphics chip make, has fixed two high-severity which can be used to view sensitive data, gain escalated privileges or launch denial-of-service (DOS) to impact Windows gaming device. One of the vulnerabilities, CVE-2020-5962, found in Nvidia Control Panel allowed attacker with local access to corrupt system file leading to DOS or escalation of privilege. CVE-2020-5963, another vulnerability in CUDA Driver, allowed code execution, DOS or information disclosure. The update also patched other eight vulnerabilities.

Source	https://threatpost.com/nvidia-windows-gamers-graphics-driver-bugs/156911/
Infected Technology	Nvidia Graphics Drivers
CVEs	CVE-2020-5962, CVE-2020-5963, CVE-2020-5964, CVE-2020-5965, CVE-2020-5966, CVE-2020-5967, CVE-2020-5968, CVE-2020-5969, CVE-2020-5970, CVE-2020-5970
Recommendation	Update to the latest patches released by Nvidia.

5. Credit card skimmer embedded in image metadata on e-commerce sites

Description	
Attackers are using malicious images injected with JavaScript, dubbed MageCart, to harvest customer sensitive details of customers. Attackers are injecting card skimmers code in EXIF metadata which is loaded in compromised e-commerce websites. The malicious image was loaded using a Wordpress e-commerce plugin according to MalwareBytes. The code within EXIF data collects the data and forwards the data to the Command and Control (C2) server as image via POST requests to conceal exfiltration of data.	
Source	https://www.zdnet.com/article/your-credit-card-information-is-now-being-stolen-through-image-files/
Infected Technology	Wordpress plugin
Recommendation	Do not use untrusted plugins Implement solutions to stay up to date with threats

6. Twitter faced data breach of Business Account

Description	
Twitter has apologized for a data breach that was identified on May 20, 2020. The data breach allowed attacker to steal data and gain access to the user account using Twitter's advertising and analytics platform. The vulnerability has been fixed by Twitter; however, the personal data of business clients may have been compromised including email address, telephone number and last four digits of credit card number.	
Source	https://cyware.com/news/twitter-apologized-on-yet-another-data-breach-of-business-accounts-d0583c84
Infected Technology	Twitter
Recommendation	Change the credentials

For any queries/recommendations:

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