May 11, 2020

INFOSEC WEEKLY

#MADE4SECURITY

- **Dark web flooded with data stolen from 11 companies**
- **DigitalOcean data leak exposed customer data**
- **Web Applications target of Blue Mockingbird Cryptomining**
- **DDOS-for-hire service SuperiorStresser operator gets suspended sentence**
- **DocuSign Phishing Campaign Uses COVID-19 as Bait**

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, Trip Advisor, 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. Dark web flooded with data stolen from 11 companies

Description	
Shine Hunters, a group of hackers, have been selling data stolen from various companies in the dark web. The group is responsible for the compromise of Microsoft' GitHub account with over 500 GB of data from its private repository and data breach of Unacademy, one of India's largest online learning platform, with over 22 Million user record. Currently, the group is selling over 150 Million user records from Tokopedia, Homechef, Bhinneka, Minted, Styleshare, Ggumim, Mindful, StarTribune, ChatBooks, The Chronicle of Higher Education and Zoosk worth more than $23,000. Some of these data contains details with email, encrypted password, current session id and other sensitive information.	
Source	https://www.bleepingcomputer.com/news/security/hacker-group-floods-dark-web-with-data-stolen-from-11-companies/
Infected Technology	Tokopedia, Homechef, Bhinneka, Minted, Styleshare, Ggumim, Mindful, StarTribune, ChatBooks, The Chronicle of Higher Education and Zoosk
Recommendation	Change the credential if account exists in above mentioned platform

2. DigitalOcean data leak exposed customer data

Description	
DigitalOcean, one of the largest web hosting platform**s**, has been recently hit by data leak. The data leak happened as a DigitalOcean-owned document from 2018 was exposed to Internet with a public link. The exposed document included customers email, name, bandwidth usage and amount paid in 2018. The document had been accessed for 15 times before taken down. The company notified the customers via email once the breach was identified. The email assured that DigitalOcean website were not compromised and credentials of the users were not exposed.	
Source	https://thehackernews.com/2020/05/digitalocean-data-breach.html
Infected Technology	DigitalOcean
Recommendation	Change the existing credentials

3. Web Applications target of Blue Mockingbird Cryptomining

Description

Researchers at security firm Red Canary uncovered a Monero cryptocurrency-mining campaign, tracked as Blue Mockingbird, that exploits the vulnerability in web applications built on the ASP.NET framework. The deserialization vulnerability could be exploited by attackers to achieve remote code execution, it affects the Progress Telerik UI for ASP.NET AJAX and was also mentioned in a joint report released by the U.S. NSA and the Australian Signals Directorate (ASD) warning of attackers increasingly exploiting vulnerable web servers to deploy web shells. This issue could be exploited only when the encryption keys are obtained via a separate attack, meaning that the attackers have to chain more exploits in their campaigns.

Source	https://threatpost.com/blue-mockingbird-monero-mining/155581/
Infected Technology	Telerik UI
CVE-ID	CVE-2019-18935

4. DDOS-for-hire service SuperiorStresser operator gets suspended sentence

Description

SuperiorStresser is a website by 20-year-old Joseph Connolly which offered range of cyber-attack services. The service offered DDOS-for-hire service to cripple websites with flooded traffic at a mere cost of £8. The operator has been captured and plead guilty. The operator has received a suspended license. Other accomplices of the service are also being investigated by the FBI.

Source	https://www.hackread.com/ddos-for-hire-service-superiorstresser-operator-suspended-sentence/
Infected Technology	
Recommendation	Ensure organization resources are equipped with visibility tools to monitor anomalies

5. DocuSign Phishing Campaign Uses COVID-19 as Bait

Description

DocuSign clients on Office 365 are the objective of another phishing effort that highlights COVID-19 as a bait to persuade them to present their qualifications as a byproduct of pandemic data. As per analysts at Abnormal Security, 50,000 to 60,000 DocuSign clients have gotten the phishing email, which indicates to be a computerized message from DocuSign conveying a connect to a COVID-related archive. The malevolent connect to the archive utilizes a three-level divert to muddle the real goal — a page that resembles a DocuSign login page. When guests are there, the aggressor takes any entered credentials.

Source	https://abnormalsecurity.com/blog/abnormal-attack-stories-docusign-phishing/
Recommendation	Always be cautious when giving off sensitive personal or account information

For any queries/recommendations:
Contact us: **whois@cryptogennepal.com**