InfoSec Weekly

Compilation of InfoSec News

Topics for the Week:

1. Dridex Malware Avoids antivirus Software Detection
2. Silence Cybergang hit Bangladesh, India, Sri-Lanka and Kyrgyzstan
3. $500,000 paid in ransomware attack dubbed "Triple Threat" paid by Florida City
4. Silex Malware in insecure IoT devices running on Linux and Unix
5. Android Malware targeting Android Devices
6. Yandex hacked by Western intelligence agencies

07/07/2019

www.cryptogennepal.com

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. Dridex malware avoids antivirus software detection

Description

A new Dridex malware has been detected having the ability to avoid detection by traditional antivirus products. Dridex is a Trojan which specializes in the theft of online banking credentials.

Source	**https://cyware.com/news/new-dridex-malware-strain-avoids-antivirus-software-detection-d93839c4**
Infected Technology	**Android**
Recommendation	**Avoid downloading applications from any unknown sources.**

2. Silence Cybergang hits Bangladesh, India, Sri-Lanka and Kyrgyzstan

Description

The Russian hackers dubbed 'Silence' were able to steal at least $3 Million from Bangladesh based Dutch-Bangla Bank via a string of cash-machine withdrawals. They were also involved with breaking into various banks' network last year.

Source	**https://www.theregister.co.uk/2019/07/03/silence_hacking_bangla**
Infected Industry	**Bank**
Recommendation	**Keep all the end-point protections and email protections up to date to avoid such incidents.**

3. $500,000 paid in ransomware attack dubbed "Triple Threat" paid by Florida City

Description	
A city in Florida has paid hackers almost $500,000 after suffering from ransomware attack which disabled its email systems and servers. The amount was paid in 42 Bitcoin to gain access to their servers.	
Source	https://threatpost.com/second-florida-city-pays-hackers-500k-post-ransomware-attack/146018/
Infection Source	Ransomware
Recommendation	Do not download and install apps from unknown sources

4. Silex Malware in insecure IoT devices running on Linux and Unix

Description	
A new malware named 'Silex' that targets Internet of Things (IoT) devices was spotted by Akamai researchers. A hacker was able to successfully brick up to 4000 insecure IoT devices before shutting down its C&C server.	
Source	https://threatpost.com/thousands-of-iot-devices-bricked-by-silex-malware/146065/
Infected Technology	IoT devices
Recommendation	If your organization is using any IoT devices, do not leave its credentials default.

5. Android Malware targeting Android Devices

Description

Security researchers revealed an ongoing Android malware campaign dubbed ViceLeaker. The malware is designed to steal sensitive information, including call recordings, text messages, photos, videos, and location data without users' knowledge. Apart from spying features, the malware also has backdoor capabilities, including upload, download, delete files, record surrounding audio, takeover camera, and make calls or send messages to specific numbers, according to the researcher.

Source	https://www.cisomag.com/new-malware-campaign-viceleaker-targeting-android-devices-researchers/
Infected Technology	**Android**
Recommendation	**Avoid downloading applications from any unknown sources.**

6. Yandex hacked by Western intelligence agencies

Description

The search engine Yandex, Russia's biggest search engine, was the target of a cyberattack that occurred late last year which was orchestrated by hackers working for Western intelligence agencies. The hackers deployed a rare type of malware, called Reign, in an attempt to spy on user accounts according to a new report from Reuters who spoke with four people familiar with the incident.

Source	https://www.techradar.com/news/russias-largest-search-engine-hacked-by-western-intelligence-agencies
Infected Organization	**Yandex**
Recommendation	**Keep all the end-point protections and email protections up to date to avoid such incidents.**

For any queries/recommendations:

Contact us: whois@cryptogennepal.com