March 23, 2020

# INFOSEC WEEKLY

## #MADE4SECURITY

- Trickbot exploits infected PCs to lunch RDP Brute force attack
- Adobe Releases Critical Patches for Acrobat Reader
- Covid-19 Themed Cyber Attack
- Multiple DDOS Botnet Exploited 0-Day flaw in LILIN DVR Surveillance System
- Mirai IoT Botnet targeting Zyxel NAS and VPN firewall
- True Fire Suffers Data Breach

CryptoGen Nepal

## 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.

**Note: During this Pandemic, we have seen a growth in cyber-attacks, and we want our viewers to be cyber aware about the fact. We have released some articles that walks you through some best practices for Employees and Organization while following Work from Home (WFH). You can find more of our articles here.**

1. **Trickbot exploits infected PCs to launch RDP brute force attack**

| Description | |
|---|---|
| A banking Trojan known as Trickbot has been in the wild since 2016 targeting financial institution across the world. Trickbot generally spreads through the email attachment which leads to fake login page. A new module dubbed "**rdpScanDLL**" has been recently discovered that lets attackers to leverage compromised system to launch brute force attacks against windows systems running a RDP connection exposed to the internet. | |
| Source | https://malwaretips.com/threads/trickbot-now-exploits-infected-pcs-to-launch-rdp-brute-force-attacks.99170/ |
| Infected Technology | Windows RDP |
| Recommendation | Create strong password with strong remote access restriction. |

2. **Adobe Releases Critical Patches for Acrobat Reader**

| Description | |
|---|---|
| Adobe has released a set of out-of-band software updates that address a total of 41 vulnerabilities in six of its products. *Adobe has released security updates for Adobe Acrobat and Reader for Windows and macOS.* Adobe inform its users of an upcoming security update for Acrobat and Reader, but the company today unveiled bugs in a total of 6 widely used software where 29 of the 41 vulnerabilities are critical in severity, and the other 11 have been rated important. | |
| Source | https://thehackernews.com/2020/03/adobe-software-update.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29 |

### 3. Covid-19 Themed Cyber Attack

| Description | |
|---|---|
| In the meantime, of a global coronavirus (COVID-19) pandemic, hackers are not letting a disaster go to waste and have now automated their coronavirus-related scams to industrial levels. Cybercriminals are now creating and putting out thousands of coronavirus-related websites daily. Most of these sites are being used to host phishing attacks, distribute malware-laced files, or for financial fraud, for tricking users into paying for fake COVID-19 cures, supplements, or vaccines. | |
| Source | https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/ |
| Recommendation | • Secure remote access technologies and use MFA<br>• Do not get tricked by any attack and watch out mail and files send by unknown sender<br>• Use trusted Source for update related to Covid-19 |

### 4. Multiple DDOS Botnet Exploited 0-day flaw in LILIN DVR Surveillance System

| Description | |
|---|---|
| Multiple 0-day vulnerability in DVR surveillance system by LILIN, a Taiwan based manufacturer has been exploited by botnet operator. The 0-day vulnerability is used to spread *Chaluba*, *FBOT*, and *Moobot*. A hard-coded login credential granting attacker ability to modify DVR's configuration file to inject backdoor command when FTP or NTP server configuration are synchronized. | |
| Source | https://blog.netlab.360.com/multiple-botnets-are-spreading-using-lilin-dvr-0-day-en/ |
| Infected Technology | LILIN DVR surveillance system |
| Recommendation | Update to the latest firmware version (2.0b60_20200207) |

### 5. Mirai IoT Botnet targeting Zyxel NAS and VPN firewall

| Description | |
|---|---|
| A new version of Mirai botnet is exploiting a critical vulnerability in Network Attached Storage (NAS) to remotely infect and control vulnerable machine. Multiple Zyxel products including NAS, UTM, VPN Firewall and ATP running firmware version up to 5.21 are vulnerable to compromise. Although Zyxel released a patch for the vulnerability with *CVE-2020-9054,* it doesn't solve the issue in many older unsupported devices. | |
| Source | https://unit42.paloaltonetworks.com/new-mirai-variant-mukashi/ |
| Infected Technology | Zyxel |
| Recommendation | Do not expose the devices on internet and tune firewall policy to prevent brute-force on device by the manufacturer |

### 6. True Fire Suffers Data Breach

| Description | |
|---|---|
| Online guitar tutoring website True Fire has apparently suffered a 'Magecart' style data breach incident that could have led to the exposure of its customers' personal information and payment card information. Confirming the breach, the notification reveals that an attacker gained unauthorized access to the company's web server somewhere around mid-last year and stole payment information of customers that were entered into its website for over five months, between August 3, 2019, and January 14, 2020 | |
| Source | https://securityaffairs.co/wordpress/99875/hacking/truefire-magecart-attack.html |
| Affected Company | True Fire |
| Recommendation | • Monitor their bank and payment card statements for any suspicious activity.<br>• User to change their credentials of True Fire Account |

**Note: During this Pandemic, we have seen a growth in cyber-attacks, and we want our viewers to be cyber aware about the fact. We have released some articles that walks you through some best practices for Employees and Organization while following Work from Home (WFH). You can find more of our articles here.**

For any queries/recommendations:

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