January 04, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- A SolarWinds Flaw that lets hackers to install SUPERNOVA Malware
- GitHub-hosted malware calculates Cobalt Strike
- Microsoft Issued a Fix for Zero-Day Six Months Ago but it Didn’t Work
- Facebook ads misused by cybercriminals to launch phishing scam
- Google Docs bug allowed hackers to view private document
- A Cross layer attacks can lead to DNS Poisoning attacks and user tracing risk
- Kaspersky Warns Against Dangerous Chrome extensions

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.

1. A SolarWinds Flaw that lets hackers to install SUPERNOVA Malware

Description

On December 25, the CERT Coordination Center reported an authentication bypass vulnerability in the SolarWinds Orion software. The authentication bypass could lead attackers to deploy SUPERNOVA malware in the target environment as a zero-day attack. The vulnerability found in the SolarWinds Orion API was used to interface Orion system monitoring and management product. The vulnerability could allow an attacker to execute unauthenticated API command to compromise SolarWinds instance remotely. Another unspecified vulnerability was reported in the Orion Platform, the platform could be used to deploy malware such as SUPERNOVA.

Source	https://www.kb.cert.org/vuls/id/843464
Infected Technology	SolarWinds Orion Platform
CVE_ID	CVE-2020-10148
Recommendation	Update the relevant SolarWinds Orion Platform • 2019.4 HF 6 (released December 14, 2020) • 2020.2.1 HF 2 (released December 15, 2020) • 2019.2 SUPERNOVA PATCH (released December 23, 2020) • 2018.4 SUPERNOVA PATCH (released December 23, 2020) • 2018.2 SUPERNOVA PATCH (released December 23, 2020)

2. GitHub-hosted malware calculates Cobalt Strike

Description

A new malware was found downloading a PowerShell script from GitHub. The malware used Word files with macros to download a PowerShell script. The execution of this script downloads a legitimate image file hosting 'Imgur' used to decode a Cobalt Strike script on Windows system. Reported by researcher Arkbird, the new malware is evasive and spawns' payloads in multifaceted steps. As the word document is opened, the embedded macro is executed that launches powershell.exe feeding the location of the PowerShell script hosted on GitHub. A PNG file is downloaded which decodes a Cobalt Strike script used to compromise devices remotely by creating shells, PowerShell script execution, privilege escalation, listening or session creation. The script also contacts with command-and-control (C2) server to receive instruction.

Source	https://twitter.com/Arkbird_SOLG/status/1343001491121065984
Recommendation	Do not open suspicious Word documents or run the macros within it

3. Microsoft Issued a Fix for Zero-Day Six Months Ago but it Didn't Work

Description

Microsoft released a patch for zero-day vulnerability in June 2020, but the company did a poor job. Security researchers from Google's Project Zero showed that attackers could still use the zero-day, despite the patch. An elevation of the privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory. An attacker who successfully exploits this vulnerability could run arbitrary code in kernel mode to install programs; view, change, or delete data; or create new accounts with full user rights.

Source	https://threatpost.com/windows-zero-day-circulating-faulty-fix/162610/
Infected Technology	Microsoft Windows 8.1 and Windows 10
Recommendation	Restrict the interaction with vulnerable service

4. Facebook ads misused by cybercriminals to launch phishing scam

Description	
The phishing campaign is executed by Facebook ads posted from pages that aim to impersonate legitimate companies in order to avoid user suspicion. There was an ad that was run that promised users 3 GB of free internet data. When the users clicked on the attached link, a Github page (static) was opened which was in essence a Facebook login lookalike phishing page. If the user was fooled, the credentials would be sent to the attackers through a Firestore database and a domain hosted on GoDaddy.	
Source	https://www.hackread.com/hackers-phish-login-credentials-with-facebook-ads/?web_view=true
Infected Technology	Facebook
Recommendation	Do not open suspicious ads in Facebook.

5. Google Docs bug allowed hackers to view private document

Description	
Google has patched a bug in its feedback tool flaw discovered by security researcher Sreeram KL on June 9th. The bug incorporated across the feedback tool that could be exploited to allow attackers to steal screenshots of sensitive Google Docs document by embedding in a malicious website. The bug was identified on 'feedback.googleusercontent.com' that allowed an attacker to modify the frame using arbitrary external website hence, letting the steal and highjack of Google Docs screenshots that were to be uploaded on the Google's server. The lack of X-Frame-Options header initiated this flaw as the change on target origin and exploiting cross-origin communication was possible.	
Source	https://thehackernews.com/2020/12/a-google-docs-bug-could-have-allowed.html
Infected Technology	Google Docs

6. A Cross layer attacks can lead to DNS Poisoning attacks and user tracing risk

Description

A new attack technique called cross layer attacks which combines vulnerabilities across multiple networks to attack the target system. The cross-layer attack is possible because the IPv6 flow label generation algorithm, UDP source port generation algorithm, and the IPv4 ID generation algorithm use the same Pseudo-Random Number Generator (PRNG). The security flaw can allow hackers to perform DNS Cache Poisoning and recognize and track Android- and Linux-based devices. It works even when the browser privacy mode is On or VPN is in use.

Source	https://arxiv.org/pdf/2012.07432.pdf
Infected Technology	Android, Linux Kernel
Recommendation	• Consider replacing the weak PRNG with stronger algorithms. • Update the Linux Kernel

7. Kaspersky Warns Against Dangerous Chrome extensions

Description

Researchers from Kaspersky said that they were able to successfully discover some of the malicious extensions on Google Chrome which can lead the attackers to abuse more than twenty browser extensions to make Chrome work for them on users' computers. Some of the popular extensions were Frigate Light, Frigate CDN, SaveFrom, etc. These extensions installed in more than 8 million users' browsers accessed a remote server in the background, trying to download malicious code

Source	https://www.kaspersky.com/blog/chrome-plugins-alert/38242/?web_view=true
Infected Technology	Google Chrome
Recommendation	• Consider disabling the malicious plugins or extensions if you are not sure how it works. • Consider using the Kaspersky or Antivirus Software.

8. Attacker are using Magecart script actively to target the popular ecommerce sites:

Description

A researcher From SanSec a Dutch Cyber Security Company found a Magecart Script where the attackers are actively using it on different ecommerce as well as several business platforms to harvest payment details on compromised stores and linked it back to the Magecart or attackers' group. Now, the attackers are using CSS code to avoid detection. Due to this, it was able to bypass detection by automated security scanners and avoid raising any flags even when examined in manual security code audits.

Source	https://cyware.com/news/magecart-active-again-with-new-multi-platform-skimmer-95273e1a
Infected Technology	Shopify, BigCommerce, Zencart, and Woocommerce
Recommendation	• Consider using two-factor authentication. • Consider using virtual cards for every financial transaction.

9. Secret Backdoor Account Found in Several Zyxel Firewall and VPN Products

Description

Zyxel has released a patch to address a critical vulnerability in its Firmware version 4.60 of Zyxel USG devices which contains an undocumented account (zyfwp) with an unchangeable password. The password for this account can be found in cleartext in the firmware. This account can be used by someone to login to the ssh server or web interface with admin privileges.

Source	https://thehackernews.com/2021/01/secret-backdoor-account-found-in.html?&web_view=true
Infected Technology	Zyxel, Zyxel Firmware
CVE	CVE-2020-29583
Recommendation	• Need to install the necessary firmware updates to mitigate the risk associated with the flaw.

For any queries/recommendations:

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