August 2, 2021

INFOSEC WEEKLY

#MADE4SECURITY

- Solarmarker malware campaigns for credential theft
- Malicious python libraries removed from PyPI portal
- Node.js fixes severe HTTP bug
- Microsoft provides more mitigation instructions for the PetitPotam attack
- LemonDuck malware patches vulnerability to retain access on network
- Linux eBPF bug gets root privileges on Ubuntu

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.

Solarmarker malware campaigns for credential theft

Description	
Researchers from Cisco Talos has identified a information and credential theft campaign by Solarmarker, a .NET based information stealer and keylogger. The malware is highly modular and is currently targeting health care, education and governments. The threat actors are suspected to be using SEO poisoning to make the dropper file available to victims based on the currently trending topics. Once infected, the malware uses a DLL file named Jupyter to steal personal information, credentials and form submission values from Firefox and Chrome. The information is then communicated via a POST request to its C2 server while complicating the attempt to analyze or decrypt the request and response.	
Source	https://blog.talosintelligence.com/2021/07/threat-spotlight-solarmarker.html
Recommendation	Do not download applications from unknown sources Monitor for IOCs provided in the source

Malicious python libraries removed from PyPI portal

Description	
Researchers from JFrog have identified eight Python packages from PyPI portal that have been downloaded for over 30,000 times to have malicious code. The packages used typo squatting to lure victims to use the malicious code in their application. The packages act as an entry point for sophisticated supply chain attack that could allow remote code execution, steal sensitive information, credentials, and access tokens for various account. The packages were removed from the portal after the team was announced.	
Source	https://jfrog.com/blog/malicious-pypi-packages-stealing-credit-cards-injecting-code/
Infected Technology	Python packages: Pytagora, pytagora2, noblesse, genesisbot, are, suffer, noblesse2, noblessev2
Recommendation	Tips for developers Confirm if the packages have been used in your developments

Node.js fixes severe HTTP bug

Description	
Node.js has released patches for a critical vulnerability that may be abused by attackers to corrupt the process and cause unexpected behavior such as application crashes and even remote code execution (RCE). The use-after-free vulnerability is to do with how HTTP2 streams are handled in the language occur when a program tries to access a resource at a memory address that has been previously freed and no longer holds the resource.	
Source	https://nodejs.org/en/blog/vulnerability/july-2021-security-releases-2/
Infected Technology	All versions of the 16.x, 14.x, and 12.x
Recommendation	Update the latest available patch.
CVE-ID	CVE-2021-22930

Microsoft provides more mitigation instructions for the PetitPotam attack

Description	
PetitPotam is the term given to a vulnerability that an unauthenticated attacker may exploit to cause a targeted server to connect to an arbitrary server and complete NTLM authentication. PetitPotam can be used in connection with an attack that targets Active Directory Certificate Services (AD CS) to gain total control of a Windows domain.Microsoft has provided more elaborate mitigation instructions for the PetitPotam attacks that were disclosed	
Source	https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/07/microsoft-provides-more-mitigation-instructions-for-the-petitpotam-attack/
Infected Technology	Windows Server 2008, Windows Server 2008 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022
Recommendation	Update latest available patch

LemonDuck malware patches vulnerability to retain access on network

Description	
LemonDuck malware, a collection of hacking tools and exploit for crypto-miner, tries to retain exclusive access to a compromised network. The malware disables anti-malware and even patches the vulnerability to prevent rival malware from compromising the network. The attacker are using multiple sites and backups to prevent the take down, attempts to disable Microsoft Defender, ESET Kaspersky and other anti-malware applications and uses outlook to spread the malware via emails with files attachments.	
Source	https://www.microsoft.com/security/blog/2021/07/29/when-coin-miners-evolve-part-2-hunting-down-lemonduck-and-lemoncat-attacks/

Linux eBPF bug gets root privileges on Ubuntu

Description	
The security researchers revealed the attack code for a high-severity privilege escalation flaw in Linux kernel eBPF, tagged as CVE-2021-3490 (Extended Berkeley Packet Filter). A local attacker may use the vulnerability to gain administrative rights on Ubuntu machines.	
Source	https://www.graplsecurity.com/post/kernel-pwning-with-ebpf-a-love-story
Infected Technology	Ubuntu 20.10 and 12.04
Recommendation	Update the latest available patch.
CVE_ID	CVE-2021-3490

For any queries/recommendations:

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

OUR SERVICES

Our services as information security company includes:


INFORMATION SECURITY AUDIT


VULNERABILITY ASSESSMENT


PENETRATION TESTING


MANAGED/CO.MANAGED SOC


INCIDENT RESPONSE


THREAT ANALYSIS


SERVER HARDENING


CYBER SECURITY CONSULTANT


INFORMATION SECURITY TRAINING

CryptoGen Nepal

https://www.facebook.com/CryptoGenNepal/
https://twitter.com/CryptoGenNepal
https://www.instagram.com/CryptoGenNepal/