February 7, 2022

INFOSEC WEEKLY

#MADE4SECURITY

- Hackers Exploited 0-Day Vulnerability in Zimbra Email Platform to Spy on Users
- Cisco fixes critical bugs in RV Series SMB routers
- New Variant of UpdateAgent Malware Infects Mac Computers with Adware
- New Malware Used by SolarWinds Attackers Went Undetected for Years
- New SEO Poisoning Campaign Distributing Trojanized Versions of Popular Software

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.

Hackers Exploited 0-Day Vulnerability in Zimbra Email Platform to Spy on Users

Description	
Attackers targeting the Zimbra open-source email platform are actively exploiting a zero-day vulnerability as part of spear-phishing attacks that began in December 2021.The espionage operation, codenamed "EmailThief," was disclosed by cybersecurity firm Volexity in a technical report released Thursday. The attacks, which began on December 14, 2021, were linked to a hitherto unknown hacker gang known as TEMP HERETIC. The zero-day problem affects Zimbra 8.8.15 open-source edition.	
Source	https://thehackernews.com/2022/02/hackers-exploited-0-day-vulnerability.html
Infected Technology	Zimbra running version 8.8.15.
Recommendation	Consider upgrading to version 9.0.0

Cisco fixes critical bugs in RV Series SMB routers

Description	
Cisco has addressed seven major security vulnerabilities affecting its RV Series routers, warning of the availability of proof-of-concept (PoC) attack code targeting some of these vulnerabilities. Aside from bypassing login and authorization, the weaknesses might be used to obtain and execute unsigned software, or even launch a denial-of-service attack. However, it did not elaborate on the nature of the vulnerability or the identification of the threat actors who may be abusing them.	
Source	https://thehackernews.com/2022/02/critical-flaws-discovered-in-cisco.html
Infected Technology	RV160, RV260, RV340, and RV345 Series routers
Recommendation	• Update to the latest version of the software.
CVE_ID	CVE-2022-20699, CVE-2022-20700, and CVE-2022-20707

New Variant of “UpdateAgent” Malware Infects Mac Computers with Adware

Description	
Microsoft revealed a previously unknown Mac malware on Wednesday, saying it has evolved since its first debut in September 2020, giving it "increasingly advanced capabilities." As one of various assault waves discovered in 2021, Microsoft's 365 Defender Threat Intelligence Team called the new malware family "UpdateAgent." However, UpdateAgent's capacity to acquire access to a device might conceivably be used to retrieve other, perhaps more harmful payloads, the researchers added. The virus is reported to spread through drive-by downloads or commercial pop-ups posing as genuine software like video apps and support agents, while the creators have steadily improved UpdateAgent to become a persistent piece of malware.	
Source	https://thehackernews.com/2022/02/new-variant-of-updateagent-malware.html
Infected Technology	MacOS
Recommendation	Install the official latest patch.

New Malware Used by SolarWinds Attackers Went Undetected for Years

Description	
Long before the scope of the attacks became clear, two complex malware families — a Linux form of GoldMax and a new implant named TrailBlazer — were installed on target systems, according to cybersecurity firm CrowdStrike. The harmful operations have since been ascribed to APT29 a Russian state-sponsored cyber espionage outfit linked to the country's Foreign Intelligence Service that has been operating since at least 2008. A Golang-based malware that serves as a command-and-control backdoor by establishing a secure connection with a remote server and executing arbitrary commands on the infected system was discovered by Microsoft and FireEye.	
Source	https://thehackernews.com/2022/02/new-malware-used-by-solarwinds.html
Infected Technology	Supply Chain of SolarWinds
Recommendation	Stay updated with latest security patches.

New SEO Poisoning Campaign Distributing Trojanized Versions of Popular Software

Description	
A persistent search engine optimization (SEO) poisoning assault has been reported, exploiting users' trust in legitimate software applications to fool them into installing BATLOADER malware on infected workstations. Attackers artificially boost the search engine ranking of websites containing their malware to make them appear at the top of search results, infecting users seeking for specific software like TeamViewer, Visual Studio, and Zoom. Mandiant also pointed up similarities between the assaults and strategies used by the Conti ransomware gang, which were made public in August 2021.	
Source	https://thehackernews.com/2022/02/new-seo-poisoning-campaign-distributing.html
Infected Technology	Search Engine Optimization
Recommendation	Do not download anything from suspicious websites.

PowerPoint Files Abused to Take Over Computers

Description	
Researchers discovered that attackers are hiding malicious executables that can modify Windows registry settings to take control of an end user's computer in an under-the-radar PowerPoint file. Attackers have been spotted sending socially engineered emails that include. attachments to ppam files with harmful purpose.	
Source	https://threatpost.com/powerpoint-abused-take-over-computers/178182/
Infected Technology	PowerPoint
Recommendation	Implement Consistent precautions to security administrators.

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/