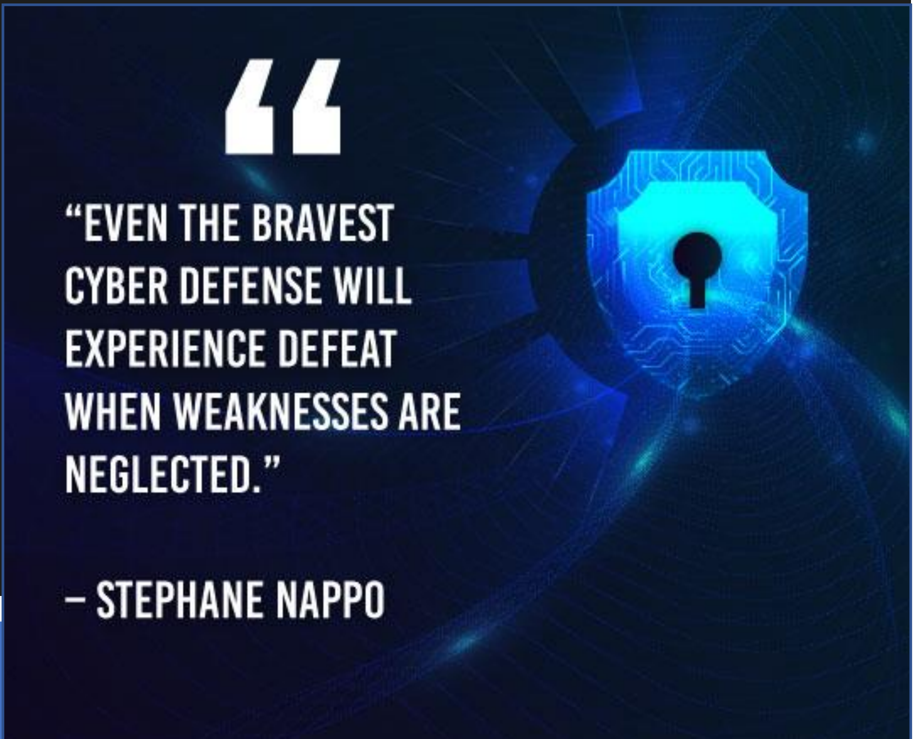
INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE -18 October 2021

Contents



"EVEN THE BRAVEST CYBER DEFENSE WILL EXPERIENCE DEFEAT WHEN WEAKNESSES ARE NEGLECTED."

– STEPHANE NAPPO

Patches Notes

EMERGENCY APPLE IOS 15.0.2 UPDATE FIXES ZERO-DAY USED IN ATTACKS

- Apple has released iOS 15.0.2 and iPadOS 15.0.2 to address a zero-day vulnerability that is being actively exploited in attacks against iPhones and iPads.
- Threat actors could potentially utilise kernel privileges to steal data or install other malware because they allow the application to execute any command on the device.

MICROSOFT OCTOBER 2021 PATCH TUESDAY

- Microsoft's October 2021 Patch Tuesday, and with it comes fixes for four zero-day vulnerabilities and a total of 74 flaws.
- Microsoft has fixed 74 vulnerabilities (81 including Microsoft Edge) with today's update, with three classified as Critical, and 70 as Important, and one as Low.

MOZILLA UPGRADES OLDER THUNDERBIRD CLIENTS

- Mozilla is rolling out a forced upgrade for Thunderbird 78.x users, getting everyone aboard version 91, the latest stable release that came out in August.
- The forced upgrade is taking users directly to version 91.2.0, released this week, and which comes with security and functional fixes.

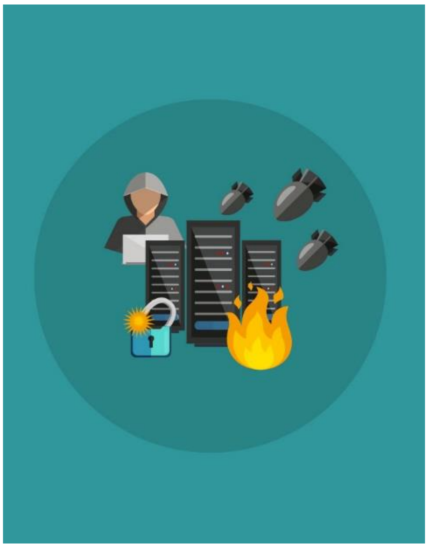
CYBER ATTACKS

INDIAN CYBER CELL'S EMAIL HACK

- MUMBAI: The email ID of the east region cyber cell of Mumbai police was hacked and phishing mails sent to other police cells with an infected PDF attachment.
- Recipients of the email have been advised by the police to not open the file as it could result in a malware infestation and thus information pilferage.

GOOGLE WARNS 14,000 GMAIL USERS TARGETED BY RUSSIAN HACKERS

- The campaign was detected in late September and accounts for a larger than usual batch of Government-Backed Attack notifications that Google sends to targeted users every month.
- In a statement sent by a Google spokesperson, Huntley says that Fancy Bear's phishing campaign accounts for 86% of all the batch warnings delivered this month.



MICROSOFT FENDED OFF A RECORD 2.4 TBPS DDOS ATTACK TARGETING AZURE

- Microsoft announced on Monday that its Azure cloud platform successfully mitigated a 2.4 Tbps distributed denial-of-service (DDoS) assault against an undisclosed European customer in the last week of August, topping a 2.3 Tbps attack.
- The attack is thought to have originated from a botnet of some 70,000 hacked devices spread across Asia-Pacific countries like Malaysia, Vietnam,

CYBERATTACK SHUTS DOWN ECUADOR'S LARGEST BANK, BANCO

- Banco Pichincha, Ecuador's largest private bank, has been hacked, disrupting operations and taking the ATM and online banking system offline.
- The bank's systems have been taken down, causing considerable disruption, with ATMs no longer working and maintenance notifications appearing on online banking portals.

Malware and Vulnerabilities

FONTONLAKE MALWARE LINUX SYSTEMS

- A new campaign has been discovered using a previously unrecognized Linux malware, FontOnLake. It provides remote access of the infected device to its operators.

- FontOnLake is a well-designed and feature-rich malware, readied by skilled and sophisticated cybercriminals. Security teams are suggested to proactively prepare their defences against this threat.

LIBREOFFICE, OPENOFFICE BUG ALLOWS HACKERS TO SPOOF SIGNED DOCS

- Updates for LibreOffice and OpenOffice have been released to fix a vulnerability that allows an attacker to make documents appear to be signed by a trusted source.

- Four researchers from Ruhr University Bochum discovered the bug, which has been assigned the number CVE-2021-41832 for OpenOffice. LibreOffice, a fork of OpenOffice developed from the original project, is affected by the same issue.

CODE EXECUTION BUG AFFECTS YAMALE PYTHON PACKAGE — USED BY OVER 200 PROJECTS

- In 23andMe's Yamale, a YAML schema and validator, a high-severity code injection vulnerability was discovered that may be easily abused by attackers to execute arbitrary Python code.

- To get around protections and execute code, the defect manipulates the schema file provided as input to the tool. The flaw is in the schema parsing function, which allows any input to be parsed and executed, which can be used for system command injection.

CYBER TECH

GOOGLE CYBERSECURITY ACTION TEAM

- The Google Cybersecurity Action Team will help protect organizations against adverse cyber events with capabilities that address industry frameworks and standards.

- Google announced the creation of its new Google Cybersecurity Action Team, which it says will have "the singular mission of supporting the security and digital transformation of governments, critical infrastructure, enterprises, and small businesses.

MICROSOFT IS DISABLING EXCEL 4.0 MACROS BY DEFAULT TO PROTECT USERS

- To safeguard customers from fraudulent documents, Microsoft will shortly start deactivating Excel 4.0 XLM macros by default in Microsoft 365 tenancies.

- Malicious campaigns that use Excel 4.0 XLM macros include TrickBot, Qbot, Dridex, Zloader, and a variety of others. For years, Microsoft has recommended that users switch from and disable Excel 4.0 XLM macros in favour of VBA macros due to their continuous abuse.

MICROSOFT REVOKES INSECURE SSH KEYS FOR AZURE DEVOPS CUSTOMERS

- Microsoft revoked insecure SSH keys some Azure DevOps have generated using a GitKraken git GUI client version impacted by an underlying issue found in one of its dependencies.

  Microsoft on September 28 that a bug in the keypair library's pseudo-random number generator led to duplicate RSA keys being generated.

MICROSOFT ADDS TAMPER PROTECTION TO WINDOWS 11 SECURITY BASELINE

- The final version of Microsoft's security configuration baseline settings for Windows 11 is now available for download via the Microsoft Security Compliance Toolkit.

- When enabling the Microsoft Security Baseline for Windows 11, administrators should make sure that the tamper protection function in Microsoft Defender for Endpoints is turned on, as it adds extra protection against human-operated ransomware attacks.

Infopercept

ABOUT INFOPERCEPT

Infopercept's vision and core values revolve around making organizations more secure through the core values of Honesty, Transparency and Knowledge, so as to enable them to make better informed decisions about their security practices & goals. With our synergistic vision to combine technical expertise and professional experience, we aim to further establish our place as a one stop shop for our clients and partners' cybersecurity and accreditation needs.

Our specialized core team comprises experienced veterans, technical experts & security enthusiasts having good practical experience & thorough knowledge in the Cybersecurity domain, latest trends, and security innovations; ensuring that you always get the best security approach & solution for your specific business needs exactly the way you want it to be.

IDENTITY ACCESS MANAGEMENT

Identity Access Management is a combination of business policies and technologies that facilitates the management of electronic digital identities. With an IAM framework in place, IT managers can control and moderate a particular user's access to critical information within an organization.

Identity and Access Management allows system administrators to utilize role based access control. This lets the administrators assign a particular role to an individual that defines his information access scope and capabilities within an enterprise's information system or networks.

Infopercept
SECURE • OPTIMIZE • STRENGTHEN
+91 98988 57117
sos@infopercept.com
www.infopercept.com

INVINSENSE™
Attacktical Cybersecurity Sense