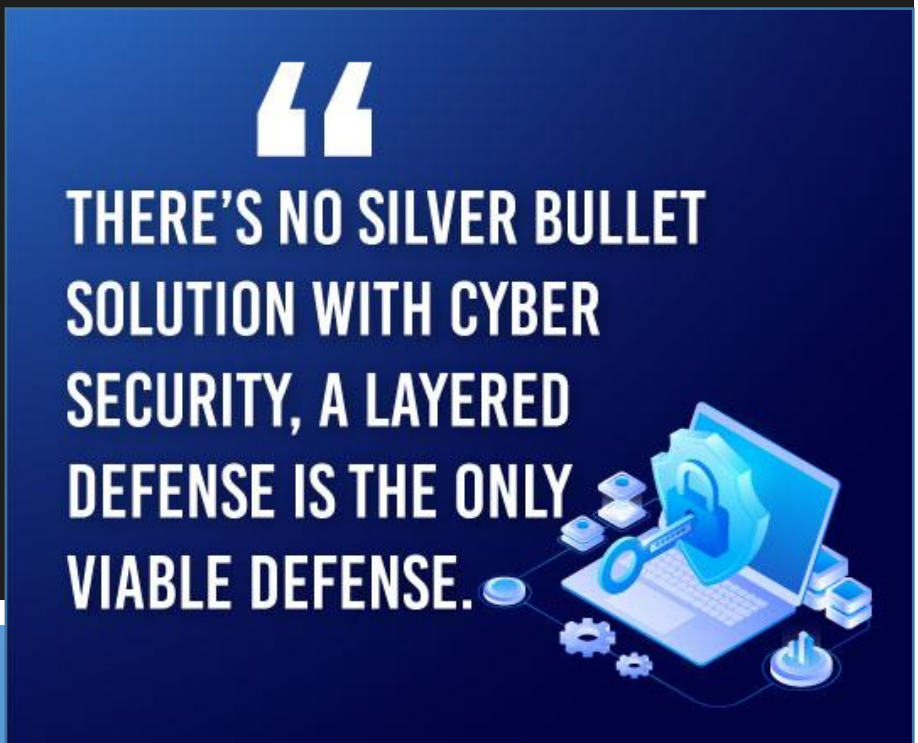
INVINSENSE™
Attacktical Cybersecurity Sense

Infopercept

INVINSENSE SECURITY AWARENESS BULLETIN

ISSUE – 11 October 2021

Contents



Patches Notes

APACHE WARNS OF ZERO-DAY EXPLOIT IN THE WILD — PATCH YOUR WEB SERVERS NOW!

- Apache users are highly recommended to patch as soon as possible to contain the path traversal vulnerability and mitigate any risk associated with active exploitation of the flaw.
- The flaw, tracked as CVE-2021-41773, affects only Apache HTTP server version 2.4.49.

ANDROID OCTOBER PATCH FIXES THREE CRITICAL BUGS, 41 FLAWS IN TOTAL

- Google released the Android October security updates, addressing 41 vulnerabilities, all ranging between high and critical severity.
- On the 5th of each month, Google releases the complete security patch for the Android OS which contains both the framework and the vendor fixes for that month.

ONIONSHARE: SECURE COMMUNICATIONS PLATFORM USED BY WHISTLEBLOWERS AND JOURNALISTS PATCHES DATA EXPOSURE BUG

- OnionShare is an open source tool across Windows, macOS, and Linux systems designed to keep users anonymous while carrying out activities including file sharing, website hosting, and messaging.
- An security team conducted an independent assessment of the software and uncovered two bugs, tracked as CVE-2021-41868 and CVE-2021-41867, which exist in versions of the software prior to v.2.4.

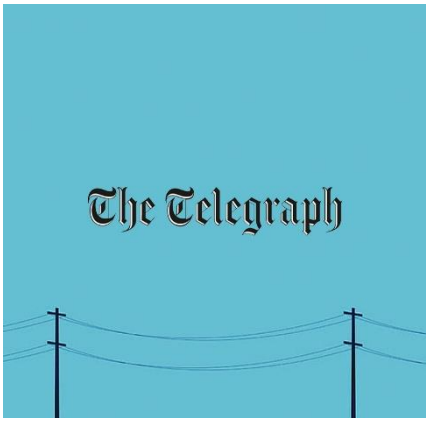
CYBER ATTACKS

MOZILLA: SUPERMAN, BATMAN, SPIDER-MAN DOMINATE LIST OF PASSWORDS

- Mozilla used data from haveibeenpwned.com to figure out the most common passwords found in breached datasets.
- Superman showed up in 368,397 breaches, Batman was featured in 226,327 breaches, and Spider-Man was found in 160,030 breaches. Wolverine and Ironman were also seen in thousands of breaches.

THE TELEGRAPH EXPOSES 10 TB DATABASE WITH SUBSCRIBER INFO

- 'The Telegraph', one of the UK's largest newspapers and online media outlets, has leaked 10 TB of data after failing to properly secure one of its databases.
- The exposed information includes internal logs, full subscriber names, email addresses, device info, URL requests, IP addresses, authentication tokens, and unique reader identifiers.



TWITCH SOURCE CODE AND CREATOR PAYOUTS PART OF MASSIVE LEAK

- Twitch appears to have been hacked, leaking source code for the company's streaming service.
- An anonymous poster on the 4chan messaging board has released a 125GB torrent, which they claim includes the entirety of Twitch and its commit history.

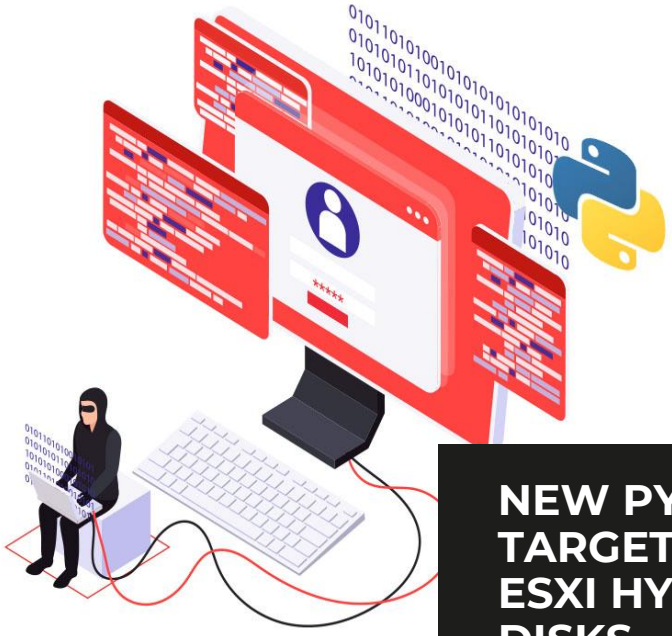
NEIMAN MARCUS SENDS NOTICES OF BREACH TO 4.3 MILLION CUSTOMERS

- Neiman Marcus, the Texas-based luxury department stores chain, is sending notices of a data breach to roughly 4.3 million customers.
- The data breach unfolded back in May 2020 when a cyber-intruder gained access to a large number of online account credentials and used them to access private customer information.

Malware and Vulnerabilities

NEW FILE-LOCKING MALWARE WITH NO KNOWN DECRYPTOR FOUND

- The ransomware, dubbed Alkhal, was likely discovered on Oct. 1 by security firms Malwarebytes and Cyclonis, which published analysis and mitigation advice on their respective websites.
- According to Malwarebytes' security guide, the Alkhal operators, who accept ransom payments in bitcoin, determine the amount based on the version of the ransomware deployed.



NEW PYTHON RANSOMWARE TARGETS VIRTUAL MACHINES, ESXI HYPERVISORS TO ENCRYPT DISKS

- The attack, one of the fastest recorded by Sophos researchers, was achieved by operators who "precision-targeted the ESXi platform" in order to encrypt the virtual machines of the victim.
- A new variant written in Python, was deployed ten minutes after threat actors managed to break into a TeamViewer account belonging to the victim organization.

MULTIPLE CRITICAL FLAWS DISCOVERED IN HONEYWELL EXPERION PKS AND ACE CONTROLLERS

- An multiple security vulnerabilities affecting all versions of Honeywell Experion Process Knowledge System C200, C200E, C300, and ACE controllers.
- The issues happen because of download code procedure which is essential to program the logic running in the controller, which enables an attacker to mimic the process and upload arbitrary CLL binary files.

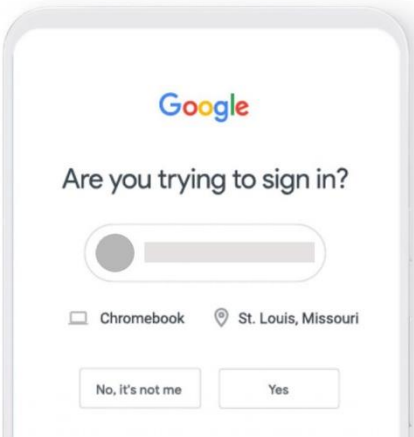
RESEARCHERS DISCOVER UEFI BOOTKIT TARGETING WINDOWS COMPUTERS SINCE 2012

- On Tuesday revealed details of a previously undocumented UEFI (Unified Extensible Firmware Interface) bootkit that has been put to use by threat actors to backdoor Windows systems
- By patching the Windows Boot Manager, attackers achieve execution in the early stages of the system boot process, before the operating system is fully loaded.

CYBER TECH

GOOGLE TO TURN ON 2-FACTOR AUTHENTICATION BY DEFAULT FOR 150 MILLION USERS

- Google has announced plans to automatically enroll about 150 million users into its two-factor authentication scheme by the end of the year.
- Google also intends to require 2 million YouTube creators to switch on the setting, which it calls two-step verification (2SV), to protect their channels from potential takeover attacks.



WINDOWS 11 IS RELEASED

- Microsoft has released Windows 11 worldwide, and it is now rolling it out via Windows Update on devices with compatible hardware and the latest updates.
- Windows 10 users can upgrade to Windows 11 for free now via Windows Update as long as their device has compatible hardware.

RHEL 8.5 IS READY FOR TESTING

- RHEL's web console, which is based on the open-source Cockpit project, now enables you to live patch the kernel from it. Previously you could only keep your Linux running while updating the kernel in real-time by using the shell.
- The updated web console also includes an enhanced performance metrics page. With this, you can more easily identify high CPU, memory, disk, and network resource usage spikes and their causes.

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.

SECURITY INFORMATION & EVENT MANAGEMENT

A Business's IT network is a goldmine of information and actionable data. At Infopercept we have a strong state-of-the-art SIEM implementation plan as well as valuable market insights due to years of experience in the Cybersecurity domain. Real time log monitoring is one of the best ways to ensure business data security and integrity.

A well suited SIEM implementation ensures the ability to systematically store, create and retrieve the logs for active Monitoring, Analysis and Compliance requirements.

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

INYINSENSE™
Attacktical Cybersecurity Sense