TOP ATTACKS AND BREACHES

- A threat actor was able to generate some mail keys of American Telecom giant AT&T, and used it to take control of AT&T customers' email addresses. Victims report that cryptocurrency accounts connected to their AT&T emails were drained, suggesting a financial motivation for the attackers.

- Microsoft warns of a recent wave in exploitation of CVE-2023-27350, a critical-severity remote code execution vulnerability in PaperCut Application servers. According to reports, the vulnerability is being utilized by threat actors to deliver the ClOP and LockBit ransomware variants. PaperCut has released a patch addressing the vulnerability.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats
  (Ransomware.Wins.Clop; Ransomware.Win.Clop; Ransomware_Linux_Clop, Ransomware.Win.LockBit; Ransomware.Wins.Lockbit)

- American cold storage and transportation company Americold has been forced to halt inbound and outbound shipping due to a cyber-attack. The company estimates that it will only be able to return to operations during the upcoming week.

- Information of 100,000 patients at the Canadian Queensway Carleton Hospital may have leaked, after a 3rd party vendor supplying communications services to the hospital had been breached. According to the hospital's statement, the information leaked includes both personal identifying information and sensitive medical history.

- Lowell city, Massachusetts, has been impacted by a cyber-attack. According to a statement by the city manager, while phones, emails and other city systems have been shut down as a consequence of the city's response to the attack, no sensitive data has been exfiltrated. In another cyber-attack against an American municipality, the South Carolina county of Spartanburg has been hit with a ransomware attack, disrupting the county's IT and phone systems.

- Hacktivist groups have targeted Israel in the past week as the country was marking its independence day. In one attack, the Iran affiliated group Sharp Boys leaked a 200,000-entry database of students' personal information breached Israeli school and college network Atid. In another attack, the group Anonymous Sudan has caused denial-of-service to multiple Israeli government, media and corporate websites.

VULNERABILITIES AND PATCHES

- VMware, cloud computing and virtualization company, has released an advisory addressing multiple vulnerabilities in VMware Workstation and VMware Fusion. The most significant vulnerability, marked CVE-2023-20869, is of critical severity, and could allow remote code execution on the host running a vulnerable version of the virtual machine.
- Code project hosting platform GitHub has patched its product to cover five security vulnerabilities, one of which allowed arbitrary code execution. According to GitHub, the vulnerabilities were reported by security researchers, and have not been observed in the wild prior to the patches' release.
- US CISA warns of multiple vulnerabilities affecting Illumina's Universal Copy Service, a medical DNA sample scanner. Successful exploitation could allow attackers full remote access to the devices to potentially alter the results of DNA samples.
- Researchers have discovered CVE-2023-29552, a new vulnerability in the network discovery protocol SLP. The vulnerability potentially allows denial of service attacks against routers by sending specific requests. The threat is deemed to be especially significant due to the high amplification factor of the denial-of-service attack, which can go above 2200 on certain routers.

THREAT INTELLIGENCE REPORTS

- Check Point Research reveals new findings related to Educated Manticore, an activity cluster with strong overlap with Phosphorus, an Iranian-aligned threat actor operating in the Middle East and North America. Educated Manticore adopted recent trends and started using ISO images and possibly other archive files to initiate infection chains

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(APT.Wins.APT35.ta)*

- Check Point Research has published its threat report for Q1 2023. According to the report, an increased amount of threats has been observed every week in comparison to Q1 2022, with organizations in the Education and Research sector seeing the highest increase in attacks. Additionally, organizations in Asia and Africa have also become increasingly targeted in 2023 as opposed to previous years.
- A campaign targeting Chinese NGO members by the Chinese APT group Evasive Panda has been investigated by security researchers. The threat group most likely used Tencent QQ, a popular Chinese social media and chat app, to deliver a backdoor to specific victims.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Infostealer.Win.PasswordStealer.A, Infostealer.Win.Generic.A)